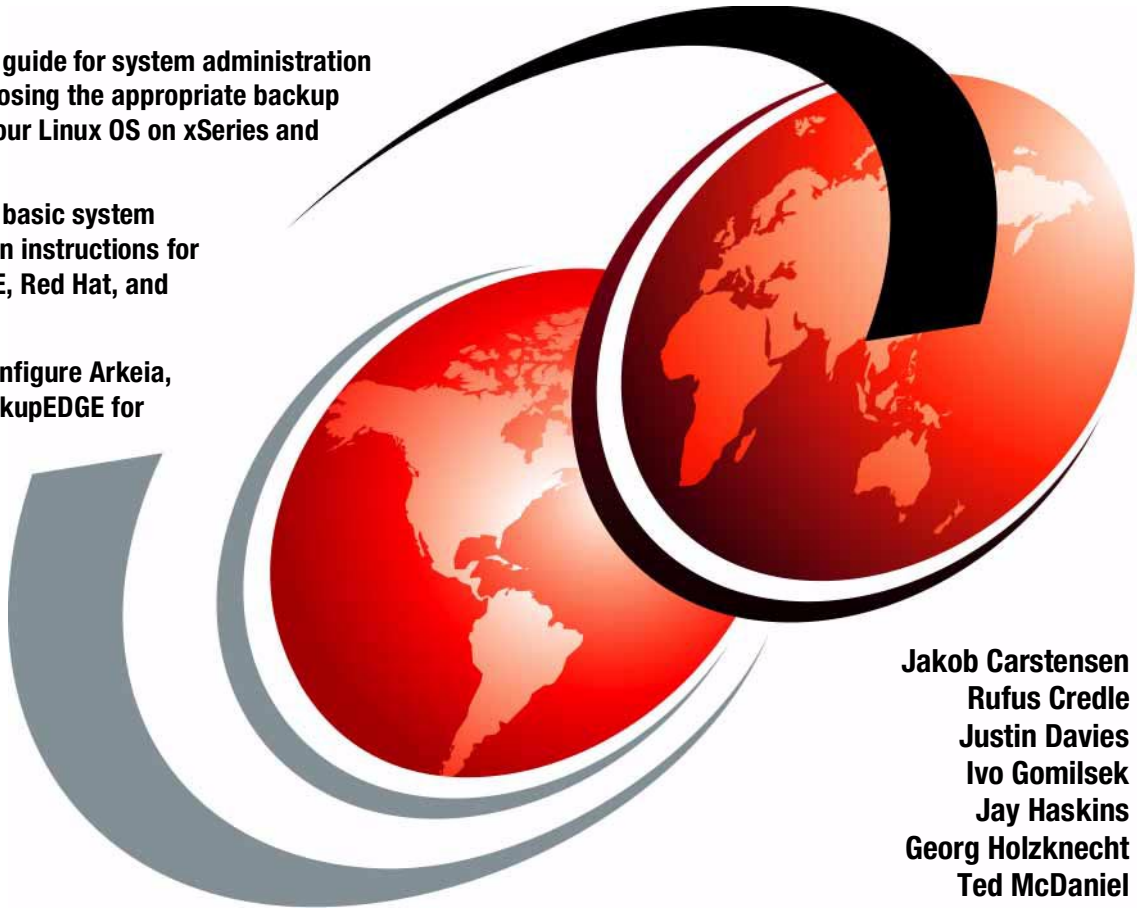
Linux System Administration and Backup Tools

for IBM eserver xSeries and Netfinity

- The complete guide for system administration tools and choosing the appropriate backup solution for your Linux OS on xSeries and Netfinity
- Step-by-step basic system administration instructions for Caldera, SuSE, Red Hat, and TurboLinux
- Install and configure Arkeia, BRU, and BackupEDGE for Linux



Jakob Carstensen
Rufus Credle
Justin Davies
Ivo Gomilsek
Jay Haskins
Georg Holzknecht
Ted McDaniel

Redbooks

ibm.com/redbooks

SG24-6228-00

International Technical Support Organization

Linux System Administration and Backup Tools for IBM @server xSeries and Netfinity

February 2001

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix A, “Special notices” on page 253.

First Edition (February 2001)

This edition applies to system administration and backup instructions of the supported Linux products: Caldera OpenLinux, Red Hat Linux, SuSE Linux, and TurboLinux on IBM @server xSeries and Netfinity servers.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. HQ7 Building 662
P.O. Box 12195
Research Triangle Park, NC 27709-2195

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 2001. All rights reserved.
Note to U.S Government Users – Documentation related to restricted rights – Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

© Copyright IBM Corp. 2001

Preface

This redbook gives you an understanding of the unified system administration incorporated in the Caldera OpenLinux, Red Hat Linux, SuSE Linux and TurboLinux operating systems. It also provides information on three Linux backup and recovery applications supported by these operating systems.

This redbook provides an understanding of Linux system administration and backup at a fairly detailed level, to help you increase your Linux skills in both areas quickly and easily.

This redbook also directs you to the available IBM Redbooks of Caldera OpenLinux, Red Hat Linux, SuSE Linux and TurboLinux that provide specific global instructions to help you plan, install, and configure each operating system on IBM @server xSeries and Netfinity for satisfactory operation.

The team that wrote this redbook

Figure 1. The team (left to right) Credle, Holzknecht, Carstensen, Haskins, Gomilsek, Davies, (lower) McDaniel

© Copyright IBM Corp. 2001

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, Raleigh Center.

Jakob Carstensen is a Technical Support Marketing Specialist in the IBM Software Group. His most recent publication was *Small Business Suite for Linux Reviewer's Guide*. Before joining the IBM Software Group, he worked at the International Technical Support Organization center in Raleigh, where he managed residencies and produced redbooks. Before joining the ITSO, he worked in Denmark both for the IBM PC Institute teaching TechConnect and Service Training courses, and for IBM PSS performing Level 2 support of Netfinity products. He has a Bachelor of Electronics Engineering degree and has worked for IBM for the past 10 years.

Rufus Credle is a Senior I/T Specialist and certified Professional Server Specialist at the International Technical Support Organization, Raleigh Center. He conducts residencies and develops redbooks about network operating systems, ERP solutions, voice technology, high availability and clustering solutions, IBM and OEM business applications, all running on IBM Netfinity and xSeries servers. Rufus's various positions during his IBM career have included assignments in administration and asset management, systems engineering, marketing and services. He holds a BS degree in Business Management from Saint Augustine's College. Rufus has been employed at IBM for 20 years.

Jay Haskins is a Systems Architect for IBM Global Services Enterprise Architecture and Design in Seattle, Washington. He has been a Linux and Open Source advocate for more than five years and currently spends most of his time developing dynamic monitoring tools using Perl and the Apache Web server. Before joining IBM, Jay worked in several different areas of the information technology field including UNIX system administration, database design and development, Windows application development, and network administration.

Justin Davies is a systems administrator and product manager at SuSE UK. He has five years of Linux experience, and his expertise is in embedded Linux systems, systems administration and network intergration. He joined SuSE in May of 2000 after graduating from the University of Derby with a diploma in computer science.

Ivo Gomilsek is an IT Specialist for Storage Area Neworks and Storage in IBM Global Services - Slovenia for the CEE region. His areas of expertise include Storage Area Networks (SAN), Storage, IBM Netfinity servers, network operating systems (OS/2, Linux, Windows NT), and Lotus Domino Servers. He is an IBM Certified Professional Server Specialist, Red Hat Certified Engineer, OS/2 Warp Certified Engineer and Certified Vinca

Co-StandbyServer for Windows NT Engineer. Ivo was a member of the team that wrote the redbook *Designing an IBM Storage Area Network, Implementing Vinca Solutions on IBM Netfinity Servers*, and the first edition of *Netfinity and Linux Integration Guide*. He also provides Level 2 support for IBM @server xSeries and Netfinity servers, and high availability solutions for IBM @server xSeries and Netfinity servers and Linux. Ivo has been employed at IBM for four years.

Georg Holzknecht is a Senior System Consultant at DeTeCSM, Darmstadt/Germany. He has 30 years of experience in different areas of the information technology field. He holds a diploma degree in electrical engineering from Technische Hochschule Darmstadt. His areas of expertise include system programming for mainframes, network operating systems (NetWare, Linux), database administration and design, application and driver development,and systems management solutions with Tivoli.

Ted McDaniel is a Senior Support Specialist at the IBM PC HelpCenter in Research Triangle Park, NC. He is the World Wide Level 2 Linux support leader for IBM x-Series and Netfinity servers. Ted has six years of experience with Level 2 support.

Thanks to the following people for their invaluable contributions to this project:

Diane O'Shea, Gail Christensen, Linda Robinson, Margaret Ticknor, and Tamikia Barrow
International Technical Support Organization, Raleigh Center

Comments welcome

Your comments are important to us!

We want our Redbooks to be as helpful as possible. Please send us your comments about this or other Redbooks in one of the following ways:

- Fax the evaluation form found in "IBM Redbooks review" on page 265 to the fax number shown on the form.
- Use the online evaluation form found at ibm.com/redbooks
- Send your comments in an Internet note to redbook@us.ibm.com

Chapter 1. System administration

You have successfully installed your Linux operating system. It is up and running. The daily life has begun. This sounds very simple, but the system administration task for setting up Linux is not considered to be that easy.

As users come and go, as data changes and grows, you have to administer your system. You have to create, modify, or delete user accounts, create and format new partitions, control permissions, and review logfiles.

New Linux users may quickly learn that it's difficult to configure their systems because the current administration system is incomplete. In fact, the Linux operating system doesn't even have an administration system at all. Linux only has a limited number of tools created by the Linux community. Because Linux does not have a complete, unified administration system, users turn to other resources (such as how-tos, man pages, and people they know), but they usually end up configuring their systems manually by editing files directly. Users shouldn't have to turn to other resources to configure their systems.

Several users around the world have created administration tools for the Linux operating system and have contributed these tools to the Linux community. However, this development process has caused some problems, including:

- The administration tools use different interfaces.
- Many administration tools are not full-featured.
- Some administration tools interfere with manual file editing.

IBM is committed to supporting the following Linux operating systems, Caldera OpenLinux, Red Hat Linux, SuSE Linux and TurboLinux. These operating systems have a complete, unified administration system to assist you and to ease administration tasks.

1.1 The adminstrative tools of Caldera, Red Hat, SuSE and TurboLinux

To administer your running system, you have a complex set of tools that is part of your operating system. But to use these tools can be quite annoying. Every tool has many very useful options, but they are rarely consistent with other tools.

The Linux distribution on IBM @server xSeries and Netfinity contains several tools that combines many administrative tasks. These tools have a

© Copyright IBM Corp. 2001

user-friendly interface, either in text mode and/or a graphical user interface (GUI).

For more information about these tools, consult the documentation that came with your Linux package. A good source for information regarding the use of these tools on IBM @server xSeries and Netfinity servers are found in the following IBM Redbooks:

- *Caldera OpenLinux Integration Guide for IBM @server xSeries and Netfinity*, SG24-5861-01
- *Red Hat Linux Integration Guide for IBM @server xSeries and Netfinity*, SG24-5853-01
- *SuSE Linux Integration Guide for IBM @server xSeries and Netfinity*, SG24-5863-01
- *TurboLinux Integration Guide for IBM @server xSeries and Netfinity*, SG24-5862-01

Using the Caldera Openlinux, Red Hat Linux, SuSE Linux, and TurboLinux tools, you can perform the following:

- Create, modify, delete user accounts and groups
- Change passwords
- Modify permissions
- Add or remove software packages
- Configure the network
- Create, modify the LILO configuration
- Modify boot mode (text mode or GUI)
- Install or remove software packages

These tools do not prevent you from using the usual UNIX tools such as passwd, adduser, fdisk, groupadd, or mke2fs, etc. or from editing system files (for example, `/etc/passwd`) manually. But since the distribution-supplied tools also check dependencies with other affected system files, your administrative work may be substantially easier.

Do not forget to monitor some important system log files:

- Red Hat Linux, TurboLinux: /var/log/messages /var/log/dmesg
- SuSELinux: /var/log/messages, /var/log/lastlog, /var/log/xferlog
- TurboLinux: /var/log

There are many books about Linux system administration from well-known UNIX and Linux book publishers. Also as part of the *Linux Documentation Project* (LDP), you can find documents that cover this area, for instance *The*

Linux System Administrator's Guide by Lars Wirzenius and Joanna Oja, or *Linux Administration Made Easy* by Steve Frampton. You can find the LDP home page at `http://www.linuxdoc.org` or `http://www.sunsite.unc.edu/LDP/`.

The Linux system administration tools available for each Linux distribution are listed in Table 1:

Table 1. Distributions and their administration tools

Distribution	Administration Tool
Caldera OpenLinux	Caldera Open Administration System (COAS)
Red Hat Linux	Linuxconf
SuSE Linux	YaST (textmode), YaST2 (GUI)
TurboLinux	turboXXXcfg (XXX: apache, fs, ftp, net, print, sound, time, user) turbohw turbopkg turboservice

1.1.1 Caldera Open Administration System (COAS)

COAS helps to improve the way users administer their Linux systems. The administration systems include the following:

- Multiple user interfaces for administration
- Modular administration tools
- Flexible, powerful administration tools
- Easy-to-use administration tools

The administration system will provide multiple user interfaces for each administration tool. Those interfaces are command line, curses, X, and Java. For more information on COAS, visit the following Web site:

`http://www.coas.org/index.html`

1.1.2 Red Hat Linux

Linuxconf is a sophisticated administration system used by the Red Hat Linux operating system. In many ways, Linuxconf is different from other administration schemes found on UNIX operating systems and most other systems.

Linuxconf is a configuration utility (a user interface to do configuration tasks) and an activator. Linuxconf is involved at different points in the operation of your Linux server or workstation. Mostly, it has features to warrant that what

you have configured is performing effectively. The different interfaces include the following:

- A text-based interface

  Linuxconf takes control pretty early at boot time when not much is enabled, especially not the X-Windows system. A text-based interface is required. This interface works on the console, on a terminal, using a Telnet session, or logged in using a simple modem.

- A Web interface

  Linuxconf may be operated with your favorite Web browser. Features of a Web browser such as bookmarks, multiple pages, and hotlinks make remote management a dream. You don't have to install an HTTPD server to get these features. Linuxconf handles the HTTP protocol itself and is started from the inetd server.

- A graphical interface

  Linuxconf has two GUI front ends. One is done in Java and is expected to operate either stand-alone or from a browser. The other is done with the wxXT toolkit and is already operational. Linuxconf is expected to evolve with some monitoring and diagnostic facilities.

- A command line interface

  The command line interface is rarely used, and in some operating systems it does not exist. During the execution of special tasks, nothing can beat a shell script. A good example is the DNS management available in Linuxconf.

1.1.3 SuSE Linux

The system administration tool used in SuSE's Linux is YaST, the acronym for Yet another Setup Tool. It is the program used to configure and administer the operating system. YaST gives you the ability to install and remove system and user software and perform basic system administration tasks. For a list of system administration activities, YaST allows you to perform the following:

- Integrate hardware into the system
- Kernel and boot configuration
- Networking configuration
- Configure the Live Filesystem CD-ROM
- Login configuration
- Set up susewm (the Windows Manager)

- User administration
- Group administration
- Create backups
- System Security Settings
- Configure XFree86
- Modify the YaST configuration file

1.1.4 TurboLinux

TurboLinux's easy-to-use TurboTools speed configuration of networks, printers, X-Windows, page updates, user accounts, and a wide variety of other system settings that ease administration once they are up and running.

These tools are featured in Table 1.

Chapter 2. Caldera OpenLinux basic system administration

This chapter will give you an overview of how to perform the most common administrative tasks on a Caldera OpenLinux eServer 2.3 operating system. Most of these tasks can be done with the Caldera Open Administration System (COAS), Caldera's OpenLinux graphical-oriented configuration and administration tool. However, you may still perform these tasks using the command-line tools.

Stop

Be careful when you are editing configuration files on your own. If you edit configuration files with an editor, make sure to maintain the format of the file. If you change the format of a configuration file, COAS may not be able to understand the configuration information and you cannot use COAS for future configuration.

2.1 Log in to the system

Before you can use any Linux system you need to log in to the system. Whenever you start Caldera OpenLinux, you will see a login window similar to Figure 2.

© Copyright IBM Corp. 2001

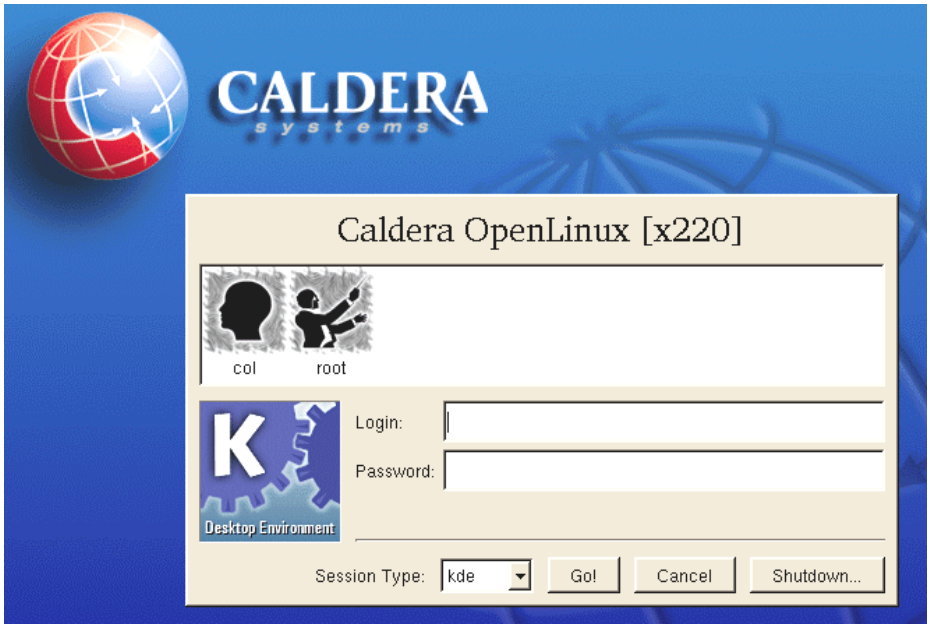


Figure 2. Login window

If you wish to use a text-based user interface, you can press Ctrl-Alt-Fx, where x is the number from 1 to 6, to switch to a text console. For example to switch to console 1, you need to press Ctrl-Alt-F1, and you will see a window similar to Figure 3.

```
Caldera OpenLinux eServer
Version 2.3
Copyright 1996-1999 Caldera Systems, Inc.


x220.first.itso.com login:
```

Figure 3. Text-based user interface

If you want to switch back to the graphical interface press Alt-F8**.** This means that you are switching to the console number 8. Caldera OpenLinux uses this console for the graphical user interface. To start working with Caldera OpenLinux, you need to log on with either a graphical or a text-based user interface. To start the graphical user interface type, in the user name and

password in the window shown in Figure 2, and click **Go!** You will see a window similar to Figure 4.

Figure 4. KDE Window Manager

2.2 Using the Window Manager

Once you are logged into the system through the graphical user interface you will see a window similar to Figure 4, which is controlled by the Window Manager. Caldera OpenLinux uses the KDE Window Manager. You can get more information about KDE on:

```
http://www.kde.org
```

At the bottom of the window you can see the toolbar that is used for accessing all available functions. It has pull-down menus, icons and buttons. You can use them for accessing the features of the operating system and applications.

Note

We recommend that you use more than 8bpp color definitions for your XFree86 server setup; otherwise, you will have problems with missing colors when you open more programs.

In the following sections we will describe how to use some basic tools in the graphical environment and especially how to customize your Caldera OpenLinux system by using COAS.

2.3 Getting the X-Windows terminal window

In order to run commands from the command line when you have the GUI Windows-based window in front of you, you need to create a terminal window. You can do this by clicking the icon representing the terminal window, circled in Figure 5.

Figure 5. Starting terminal window

After the terminal window is started, you will see a window similar to Figure 6.

Figure 6. Terminal window in KDE

In this terminal window you can access the system from a command-line prompt as in a text-based interface. The command line prompt gives you more flexibility than menus, but you can do most of the basic things from the menu system. It is a matter of personal choice.

2.4 Accessing COAS - Caldera Open Administration System

All the administration tasks in Caldera OpenLinux are performed through the use of COAS. You can access the COAS tools by clicking the **COAS** icon on the KDE toolbar, circled in Figure 7.

Figure 7. Accessing the COAS tools

After you click the **COAS** icon, you will see a window similar to Figure 8.

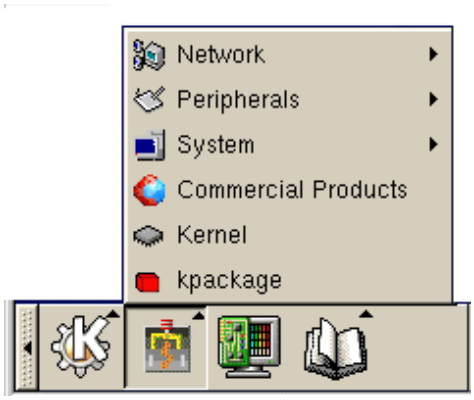


Figure 8. COAS tools

You can see you have several tools available. We will discuss them in the following sections.

2.5 Adding and removing software packages using kpackage

If you want to add or remove software once Caldera OpenLinux is installed or just check if the software is installed, you can do this by using the kpackage tool. You can start kpackage by selecting **kpackage** from the COAS tools menu, as you can see in Figure 9.

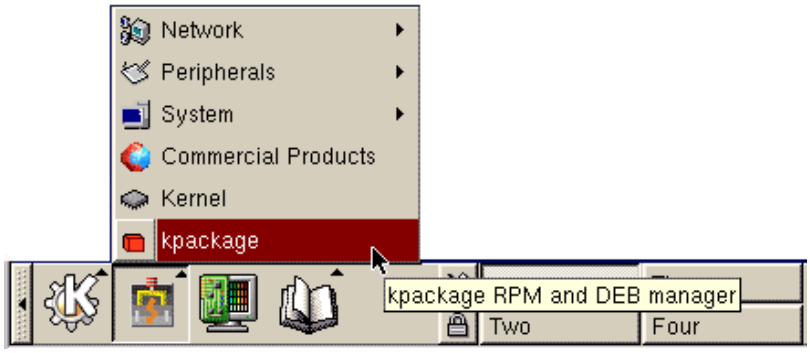


Figure 9. Starting kpackage

When kpackage is started, you will see a window similar to Figure 10.

Figure 10. kpackage

2.5.1 Uninstalling a package

If you want to uninstall a package, select the desired package and click **Uninstall.** You will see a window similar to Figure 11.

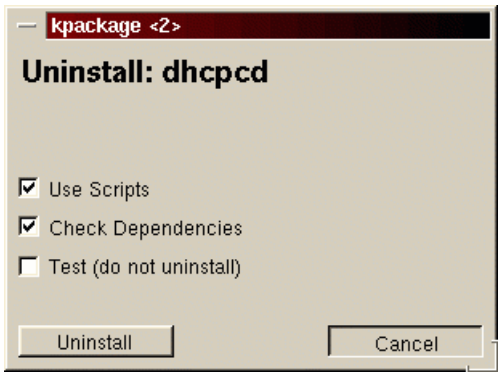


Figure 11. Uninstalling a package

Before you uninstall a package, you can change the options, but we suggest that you leave the default settings unchanged. After you have adjusted the settings, click **Uninstall** to continue. After the dependencies are checked, the package will be uninstalled.

2.5.2 Installing a package

To install a package, click **File > Open**, and you will see a window similar to Figure 12.

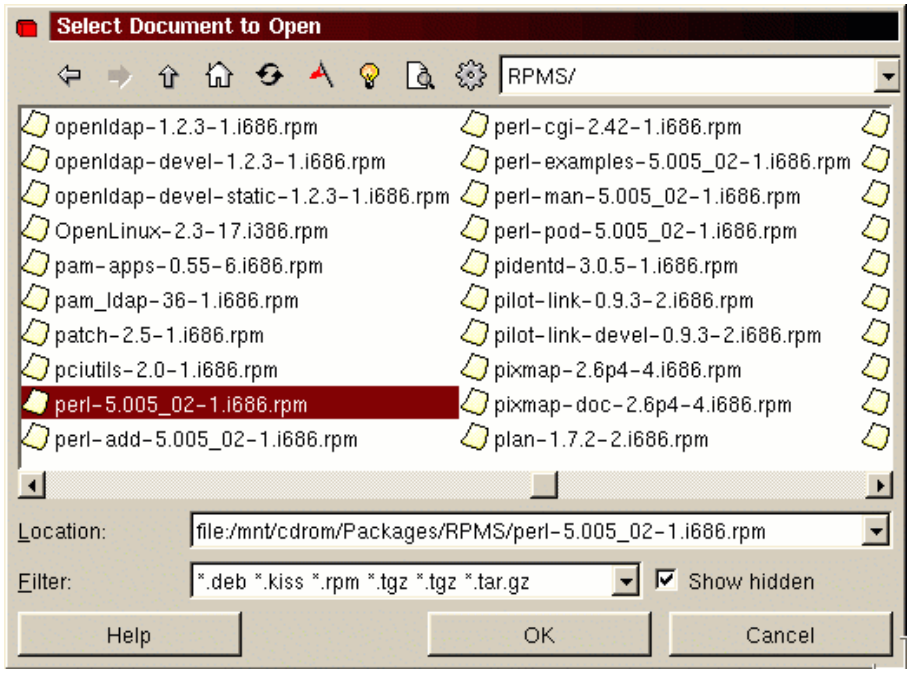


Figure 12. Selecting a package to install

Here you can select the packages you wish to install from any available system directory.

Note

If you want to install packages from a CD-ROM, you must mount the CD-ROM drive before you can access the files on it. This can be done with the command `mount /mnt/cdrom` from a command prompt.

After you have selected the package, click **OK** to continue. You will see a window similar to Figure 13.

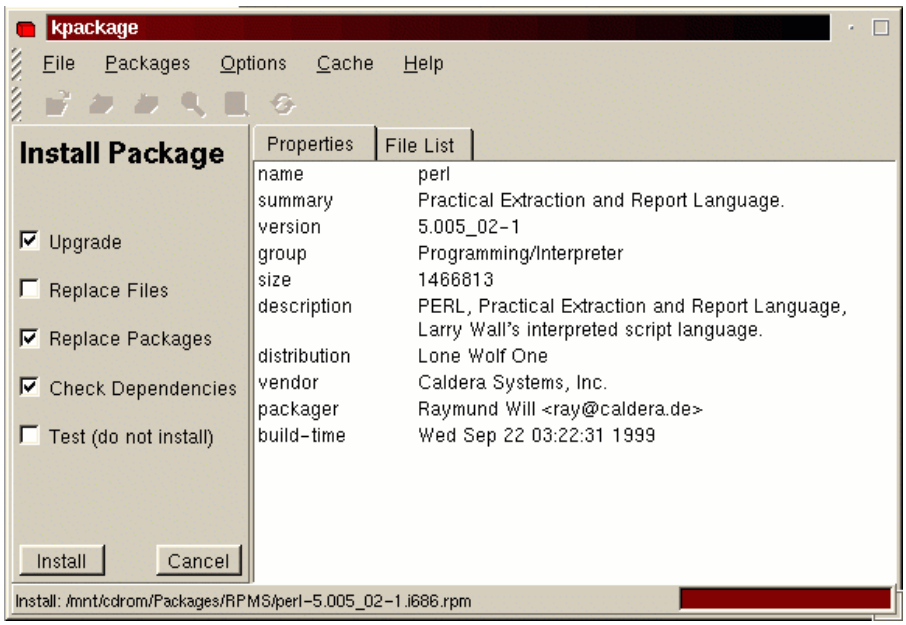


Figure 13. Description of a new package

In this window you see the description of the package. Select the **File List** option to see which files are included with the package. Before you actually install packages, you can adjust the installation options. The options are:

- **Upgrade** - this is used if you are installing a package that is already installed
- **Replace File** - if there are files in the same location already, they will be replaced automatically
- **Replace Packages** - packages are updated in the packages database
- **Check Dependencies** - check if all dependencies are satisfied
- **Test (do not install**) - perform a test installation

After you have selected your options, click **Install** to install the package. After the package is installed it will appear in the package list, as you can see in Figure 14.

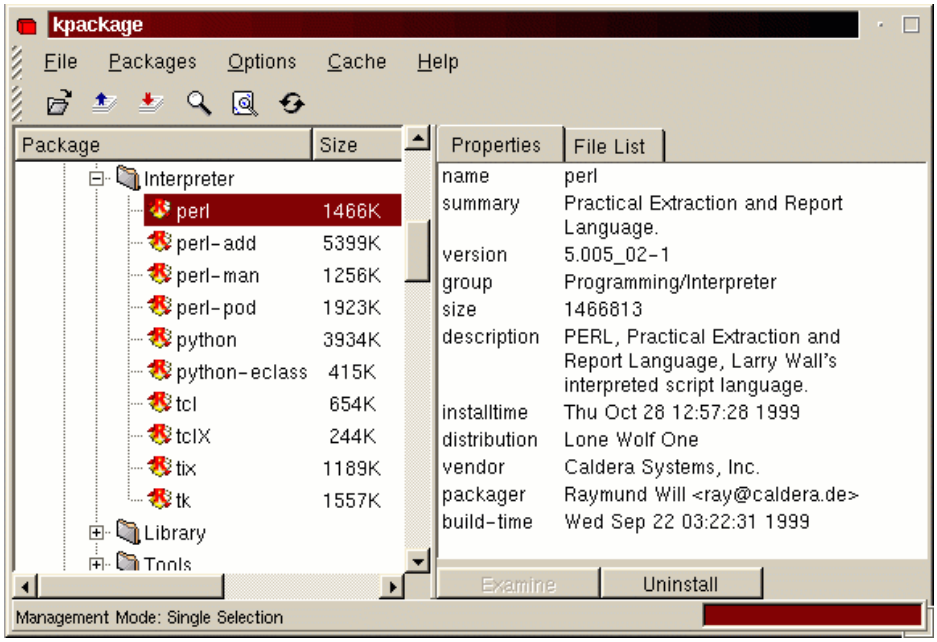


Figure 14. After the installation

2.6 Package management using RPM

Package management can also be done directly with the Red Hat package manager (RPM) package manager on the command line. The command line in the graphical interface can be accessed through the terminal window as we described in 2.3, “Getting the X-Windows terminal window” on page 10. Table 2 shows some of the most frequently used versions of the RPM commands.

Table 2. Basic RPM commands

Command	Description
`rpm -q <package>`	If a package is installed, check version and build number of the installed package.
`rpm -qi <package>`	Obtain more information about an installed package.
`rpm -qa`	List all installed packages.
`rpm -qf <filename>`	Determine the (installed) package that `<file>` belongs to.

Command	Description
`rpm -Uhv <package.rpm>`	Update/Install the file `package.rpm` showing a progress bar.
`rpm -F -v ./*.rpm`	Update (freshen) all currently installed packages using the RPM files in the current directory.
`rpm --help`	Get help about the different options and parameters.

Note

After you install packages using RPM, you may need to run some additional configuration programs. Programs such as Apache need to be customized to your particular environment and require some post-installation maintenance. Some of these packages can be configured from the graphical interface by selecting other icons. Other packages have their own configuration tools.

More information and options about RPM can be found in the manual page (man rpm), the RPM how-to file (less /usr/doc/howto/en/RPM-HOWTO.txt.gz) and at the RPM Web site at `http://www.rpm.org`. You can also display a short overview by running `rpm --help`..

2.7 System menu

In the System menu of the COAS tools, you can access the following tools:

- Accounts - for managing the accounts
- Daemons - for managing the startup programs
- Filesystem - for mounting devices and NFS volumes
- Hostname - for setting hostnames
- Resources - for checking the hardware resources
- Time - for setting the time and time zone

The System menu is shown in Figure 15.

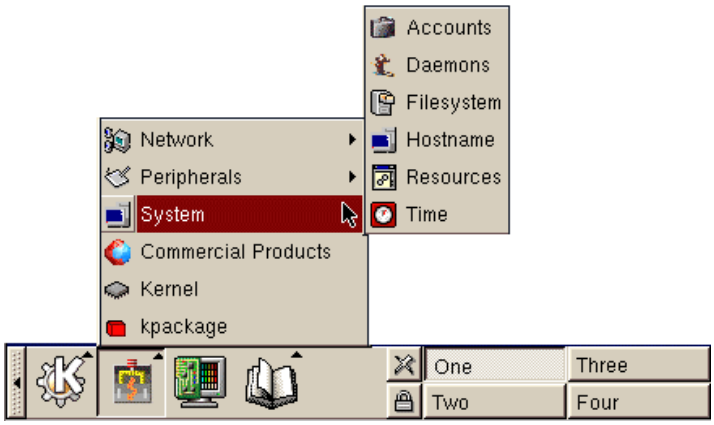


Figure 15. System menu

To start the tools from the System menu, select the tool you want. At the initial window, click **OK** to continue.

2.8 Accounts

This tool is used to manipulate the user accounts. After the tool is started, you will see a window similar to Figure 16.

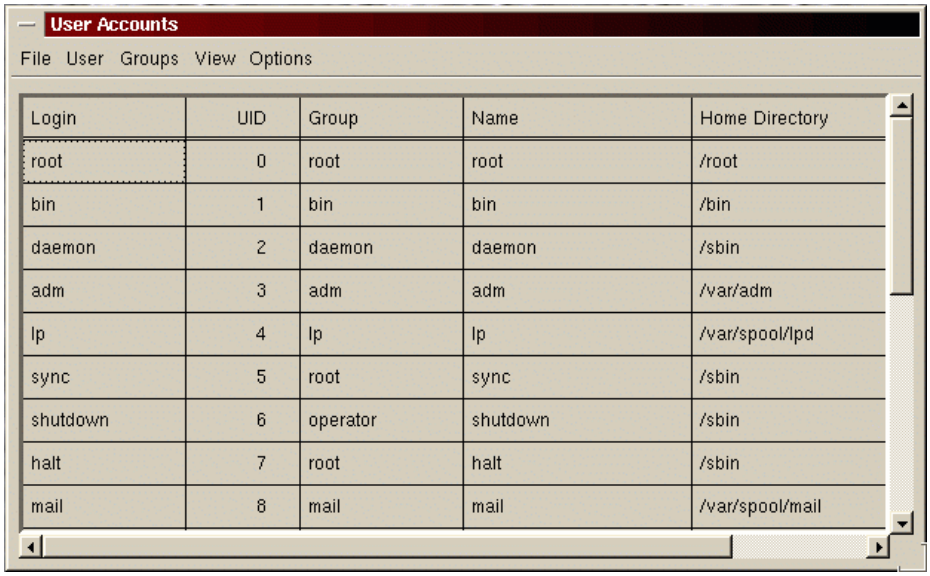


Figure 16. Account management

Here you can manage users and groups. In the following sections we will describe how to perform these tasks.

In the View menu, you have two options for displaying users:

- All users - all users will be displayed
- Regular users - only regular users will be displayed

In the Options menu, you have three options to choose from:

- Preferences - here you define the global preferences for creating users and groups. If you select this option you will see a window similar to Figure 17.

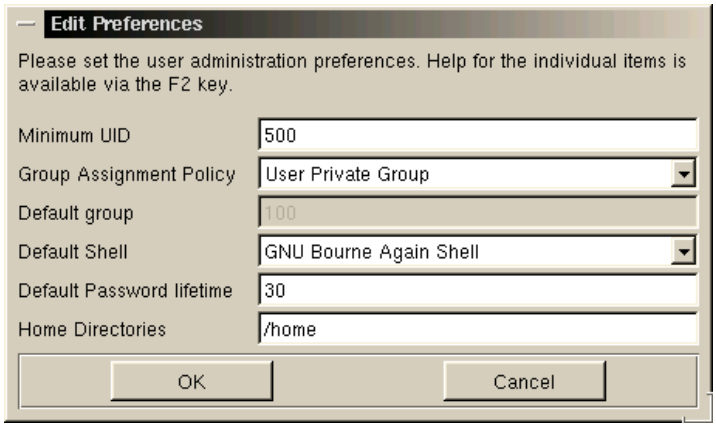


Figure 17. Setting the preferences for creation

Define your preferences and click **OK** to store them.

- Enable/Disable shadow passwords - here you can enable or disable shadow passwords.
- Enable/Disable NIS lookups - here you can enable or disable NIS lookups.

2.8.1 Managing accounts

In this section we explain how to manage accounts. We cover adding a new user, deleting a user and editing an existing user.

To create a new user follow these steps:

1. To add a new user, select **User > Create User**. You will see a window similar to Figure 18.

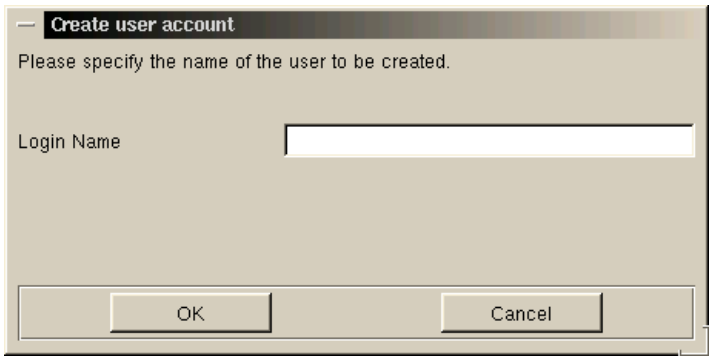


Figure 18. Login name for the new user

2. Type in the unique login name of the new user and click **OK** to continue, and you will see a window similar to Figure 19.

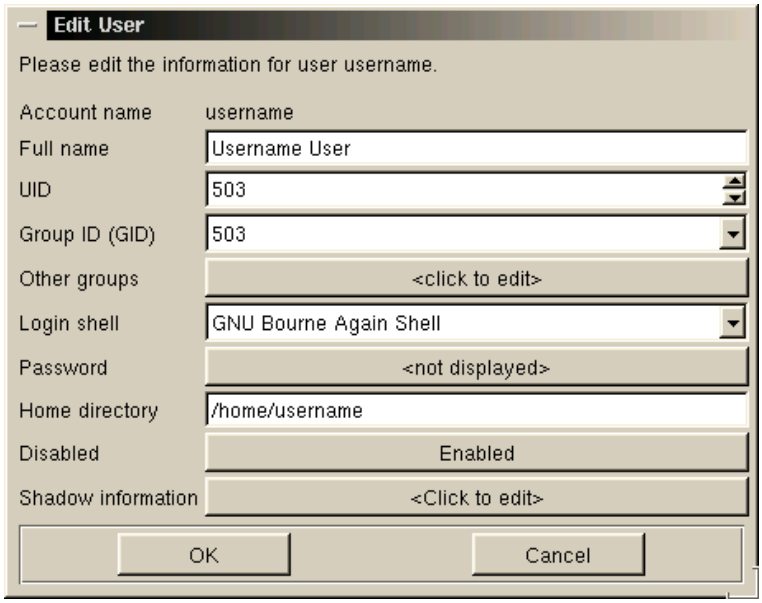


Figure 19. Specifying parameters for the new user

Here you need to specify the following:

- **Full name** - this is the description of the user
- **UID** - this is the number by which the system knows you. It only attaches this number to file and directory ownership and uses /etc/passwd to convert this to a username when listing the attributes. Generally UID numbers are unique and the system programs will usually prevent you from creating more than one username with the same UID. This can usually be overridden by specifying options to the commands to create IDs.
- **GID** - this is a unique number assigned to a group. In Caldera OpenLinux each user has its own default group. The default GID is the next available and the GID numbers are starting at 500.
- **Other groups** - each user can be a member of one or more groups. You can specify these groups here. If you click the button you will see a window similar to Figure 20.

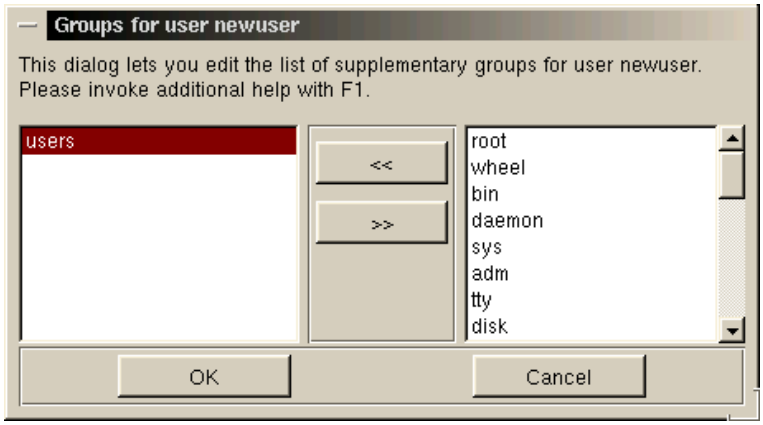


Figure 20. Specifying other groups for the user

When you have added all the groups you want, click **OK** to continue.

- **Login shell** - the shell that is started when the user logs in.
- **Password** - the password used to log in with. To define a password, click the button labeled **<not displayed>** and you will see a window similar to Figure 21.

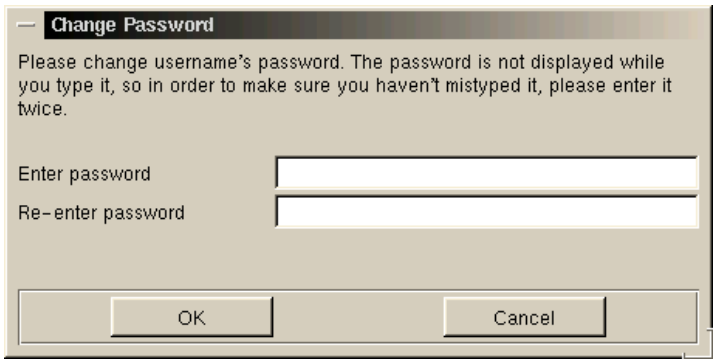


Figure 21. Specifying the password for the new user

Type in the password for the user and click **OK** to continue.

Note

Caldera OpenLinux uses shadow passwords by default.

- **Home directory** - this is the user's home directory. It is the first place a user goes to when logging in. It contains files and programs that are owned and used by that user.
- **Disabled/Enabled** - with this you define if an account is enabled or disabled. You can toggle this value by clicking the button.
- **Shadow information** - here you define the password properties: expiration, change timeframe, etc. If you want to change the default values, click the button and you will see a window similar to Figure 22.

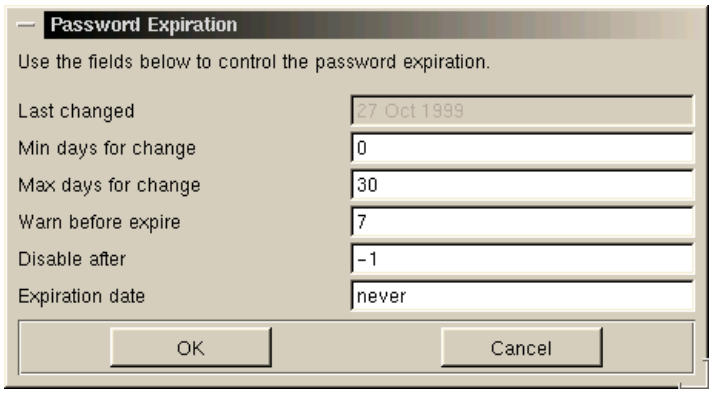


Figure 22. Password properties for the new user

When you have edited the properties, click **OK** to save them.

3. After you have typed in all necessary information for the new user, click **OK** to actually create the new user.

2.8.1.1 Deleting a user

When you want to delete a user, select the user from the list and click **User > Delete User**. You will see a window similar to Figure 23.

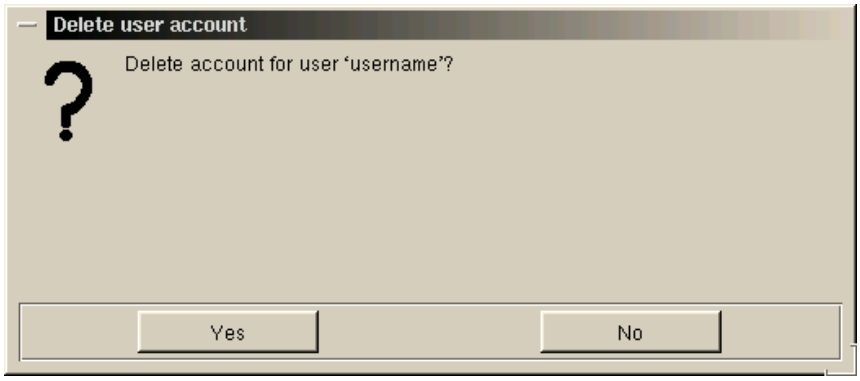


Figure 23. Deleting a user

Click **Yes** to delete the user.

2.8.1.2 Editing a user

When you want to edit a user, select the user from the list and choose **User > Edit User**. You will see a window similar to Figure 24.

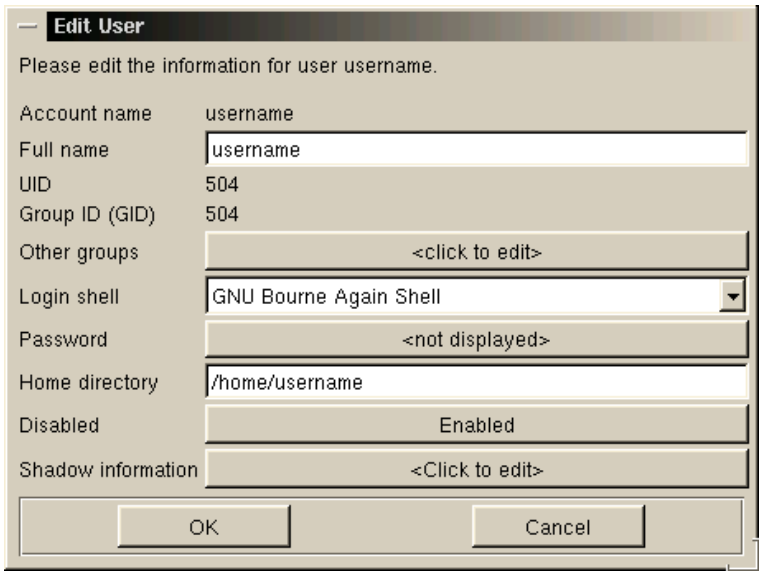


Figure 24. Edit a user

Here you can modify the following attributes of a user:

- Other groups
- Login shell

- Password
- Home directory
- Disabled/Enabled
- Shadow information

We described these attributes in 2.8.1, “Managing accounts” on page 21. When you are done, click **OK**.

2.8.2 Managing groups

You can access the tool for managing groups by selecting **Accounts > Groups > Manage groups**. You will see a window similar to Figure 25.

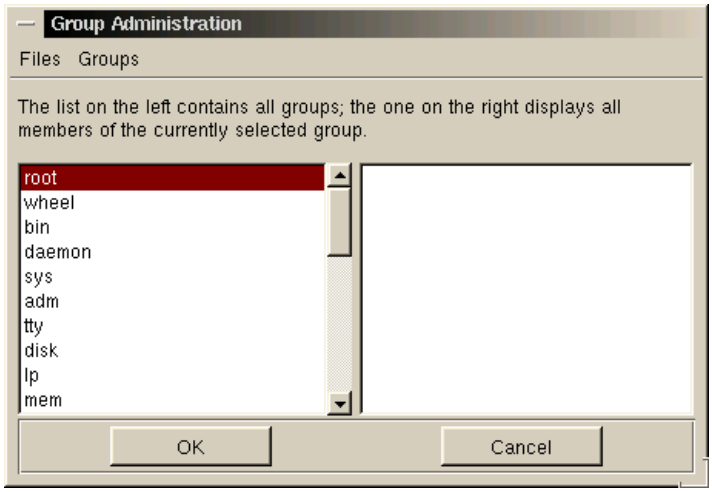


Figure 25. Group Administration

Here you can perform operations related to the groups.

2.8.2.1 Creating a new group

You can create a new group by selecting **Groups > Create Group**. You will see a window similar to Figure 26.

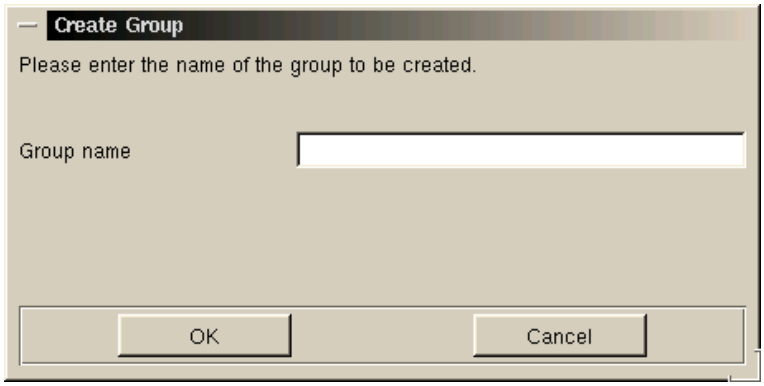


Figure 26. Creating a new group

Type in the name of the new group and click **OK** to create it.

2.8.2.2 Deleting a group

Select the group you want to delete from the list of all the groups and choose **Groups > Delete Group**. You will see a window similar to Figure 27.

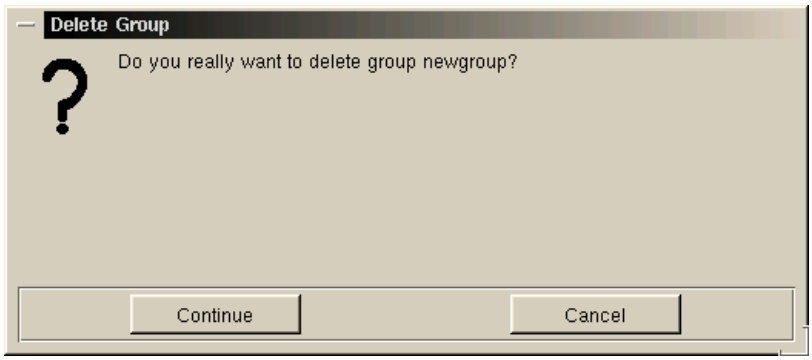


Figure 27. Deleting a group

Click **Continue** to actually delete a group.

2.8.2.3 Rename a group

Select the group you want to rename from the list of all the groups and choose **Groups > Rename Group.** You will see a window similar to Figure 28.

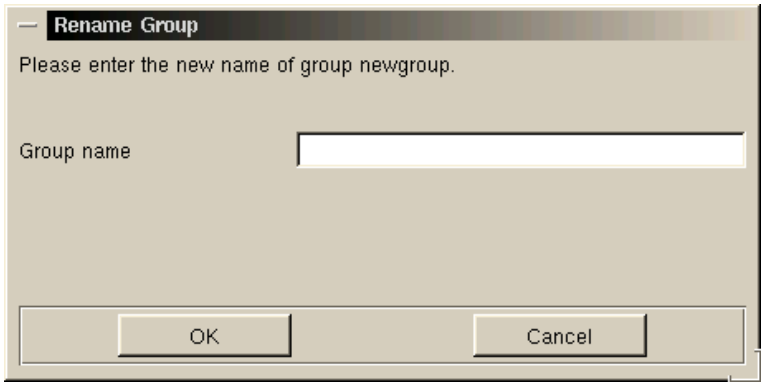


Figure 28. Renaming a group

Type in the new name for the group and click **OK** to rename it.

2.8.2.4 Merge a group

You have the option to merge users from one group to another. Select the group to which you want to merge another and choose **Groups > Merge Group**. You will see a window similar to Figure 29.

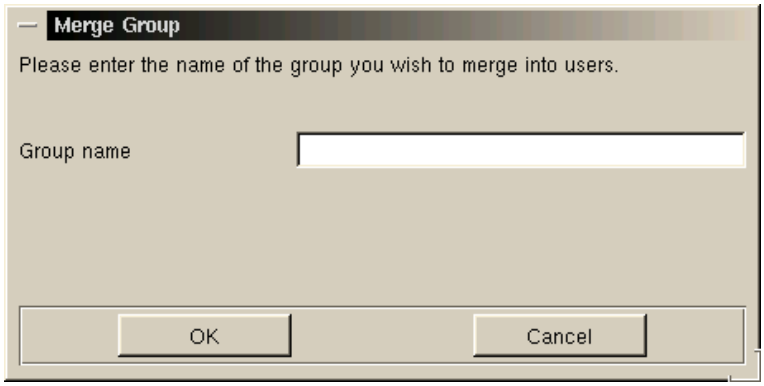


Figure 29. Merge a group

Type in the name of the group you want to merge in. Click **OK** to continue.

2.8.2.5 Group membership

You can change the members of a group. To change the members of a desired group select the group from the list of all the groups and choose **Groups > Group Membership**. You will see a window similar to Figure 30.

Figure 30. Group membership

You can add or remove users from a group. Click **OK** to save your changes.

2.9 Daemons (services)

This tool is used to manipulate the daemons that will start at the server startup. After the tool is started you will see a window similar to Figure 31.

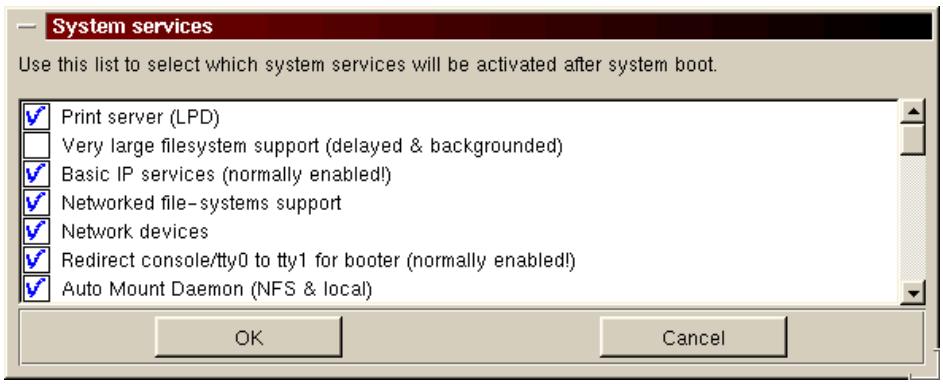


Figure 31. System services

Here you define which services (daemons) will be started at the server startup. When you are finished, click **OK** to save your changes.

2.10 Filesystem

Here you can mount or unmount the devices and connect to the NFS servers. After the tool is started, you will see a window similar to Figure 32.

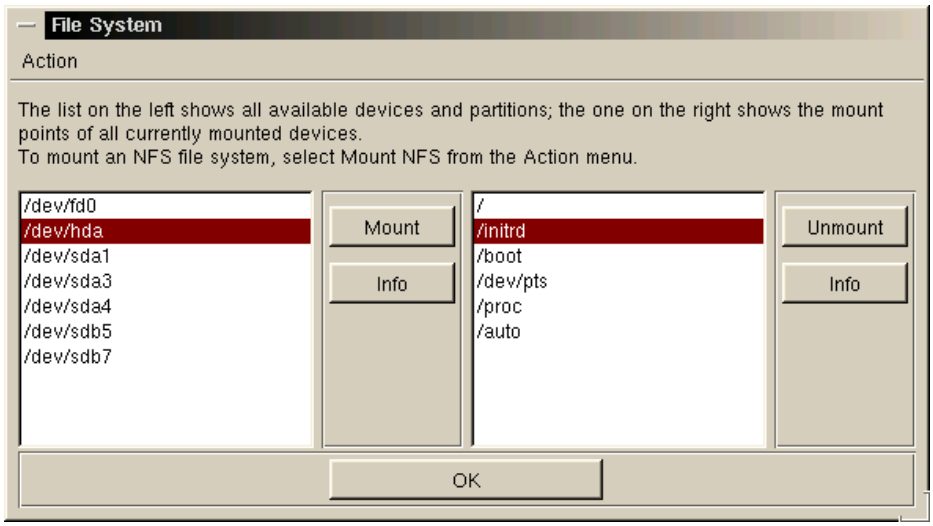


Figure 32. Filesystems

On the left side you see unmounted devices. If you want to mount the device, select it from the list and click **Mount.**

On the right side you see mounted devices. If you want to unmount an already mounted device, select it from the list and click **Unmount.**

By selecting the mounted or unmounted device and clicking **Info,** you will see the information about the particular device.

2.10.1 Mounting an NFS volume

You can mount an NFS file system by choosing **Action > Mount NFS**. You will see a window similar to Figure 33.

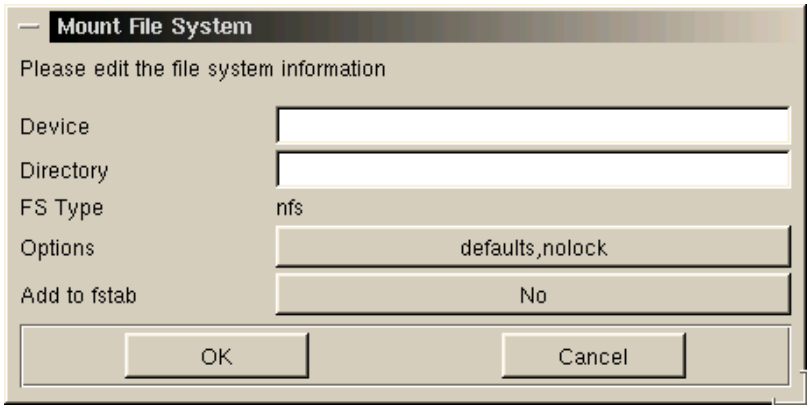


Figure 33. Mounting an NFS volume

Type in the required values and click **OK** to mount the NFS volume.

2.11 Hostname

Here you can change the hostname of your Linux server. After the tool is started you will see a window similar to Figure 34.

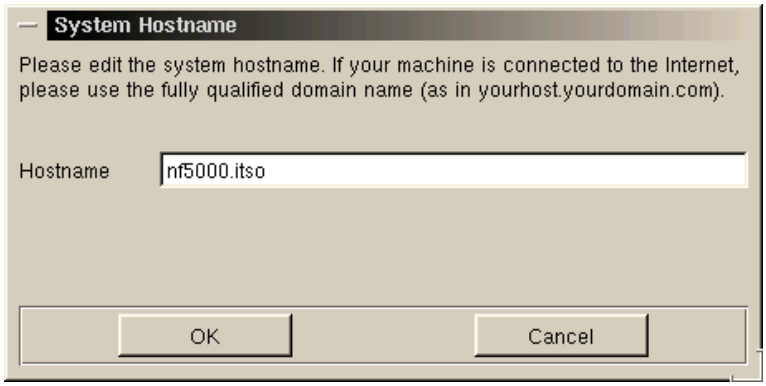


Figure 34. Changing the hostname

Type in the new hostname and click **OK** to save it.

2.12 Resources

With this tool you can examine hardware resources. After the tool is started you will see a window similar to Figure 35.

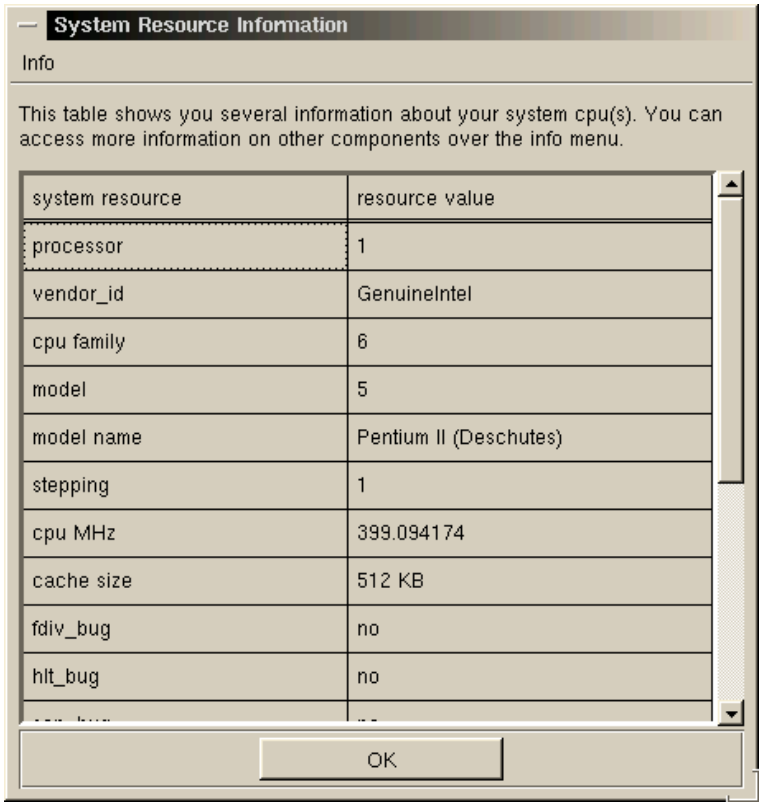


Figure 35. System resources

Here you can get information about the following resources:

- Block devices
- Character devices
- Interrupts
- System load average
- IOports
- DMA

To access this information, select the appropriate option from the Info menu. For example if you select **Interrupts**, you will see a window similar to Figure 36.

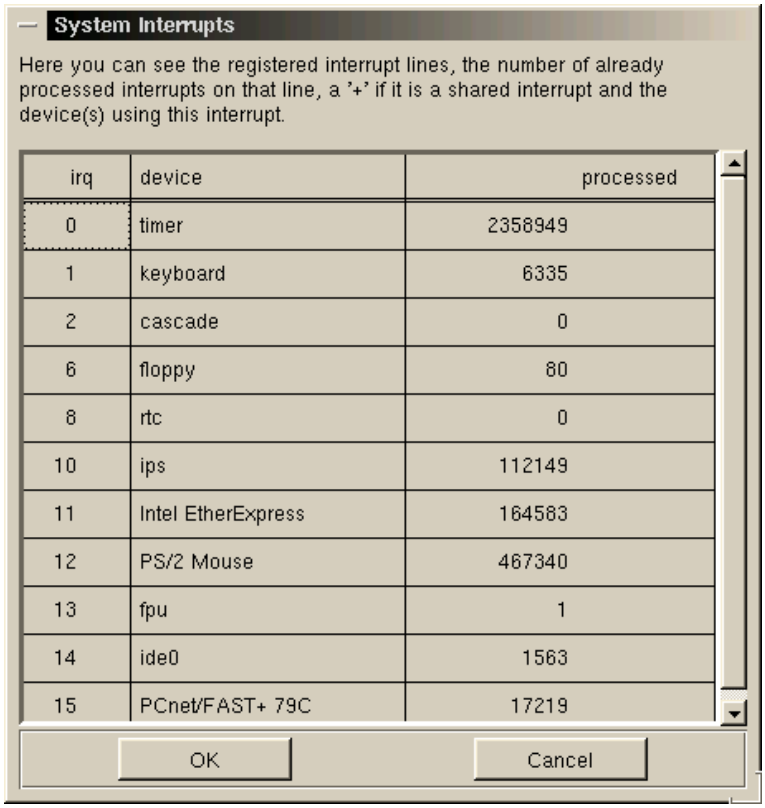


Figure 36. System interrupts

2.13 Time

Here you can set the time and time zone. After the tool is started, you will see a window similar to Figure 37.

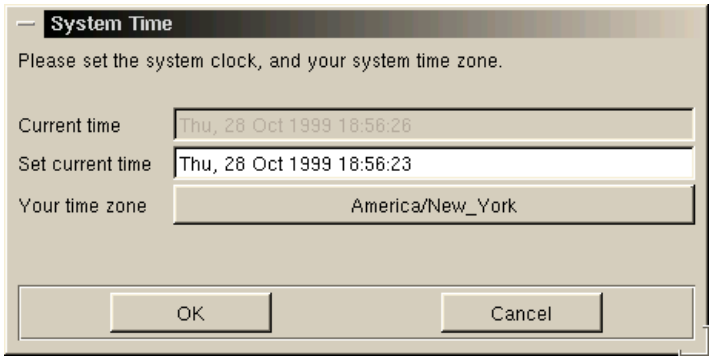


Figure 37. Setting the time

Type in the current time. If you also want to change the time zone, click the button for it. You will see a window similar to Figure 38.

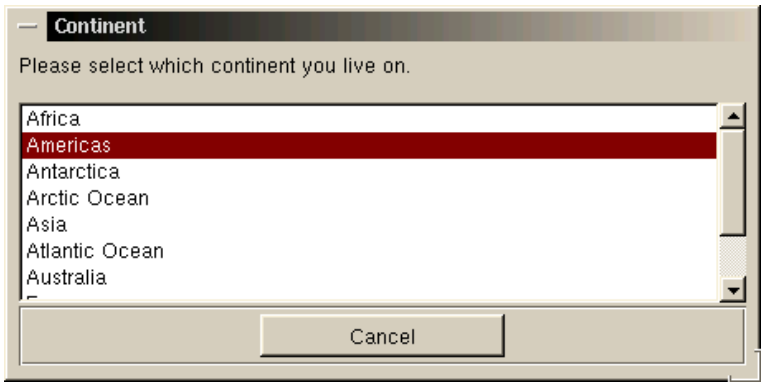


Figure 38. Setting the time zone

Select your region and you will be presented with the time zones for that region. Select the one that matches your city. After that you will be back in the System Time panel. Click **OK** to save the changes.

2.14 Peripherals menu

In the Peripherals menu of the COAS tools you can access the following tools:

- **Mouse** - for managing the mouse
- **Printers** - for managing the printers

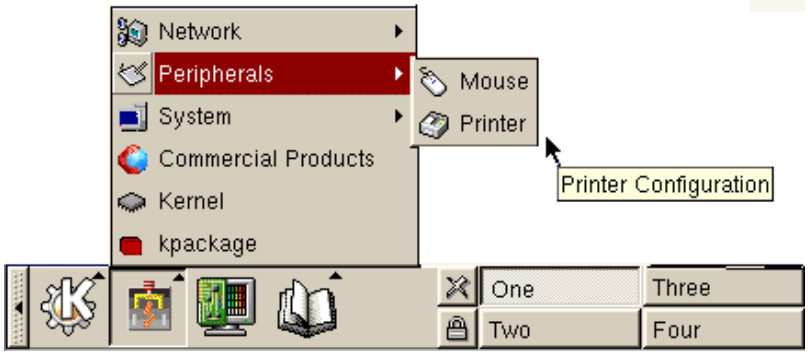


Figure 39. Peripherals menu

To start the tool from Peripherals menu, select the tool you want. At the initial dialog, click **OK** to continue.

2.15 Mouse

This tool is used to configure the behavior of the mouse in the text-based user interface. After the tool is started you will see a window similar to Figure 40.

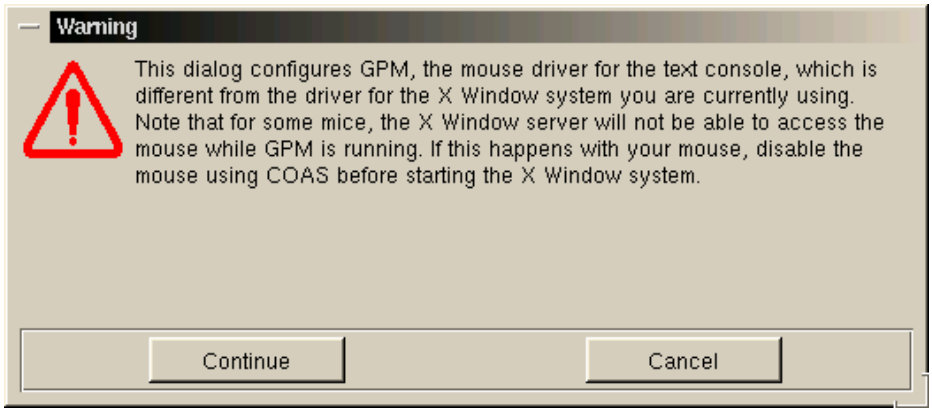


Figure 40. Warning before configuring the mouse

As you can see from the warning, this tool is used for configuring the GPM to enable additional features for mouse usage in the text-based interface. Click **Continue** to continue with the configuration. You will see a window similar to Figure 41.

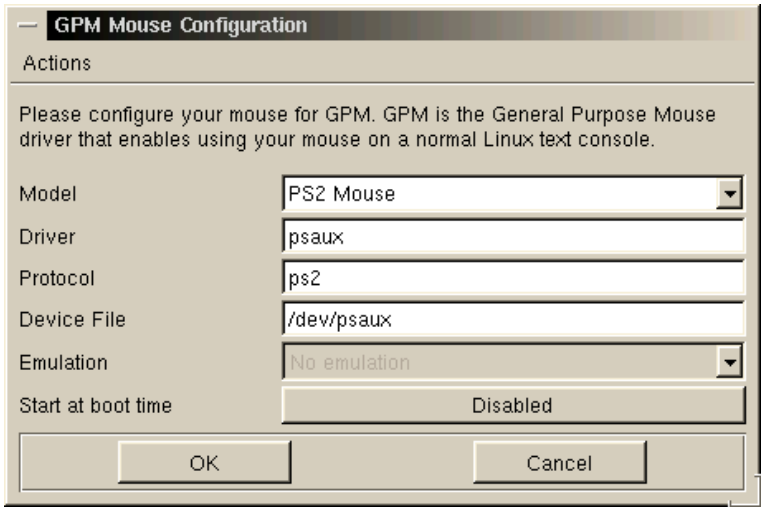


Figure 41. GPM Mouse Configuration

Select the configuration parameters that meet your needs and click **OK** to continue. On the next window, click **Save** to save your settings.

Note

If you did not install the GPM package, you will receive the error message that the daemon cannot be started.

2.16 Printer

This tool is used to configure the printers you want to use in your Caldera OpenLinux system. After the tool is started, you will see a window similar to Figure 42.

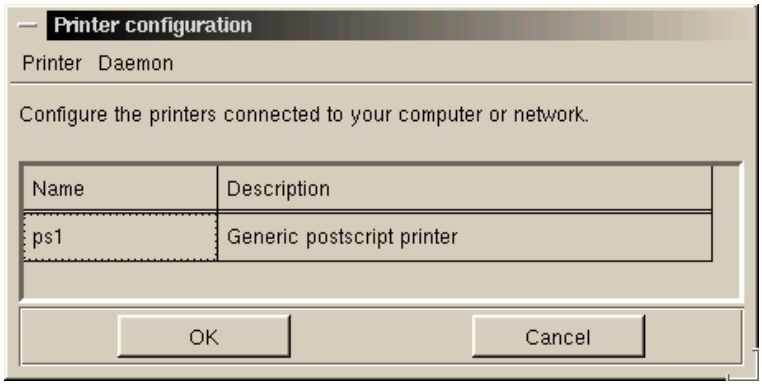


Figure 42. Printer configuration

Here you can manage printers. In the following sections we will describe how to perform these tasks.

From the Daemon menu you can start or stop the printer daemon.

Note

You can only print documents if the daemon is running.

2.16.1 Adding a new printer

You can add a new printer to your system by selecting **Printer > Add**. You will see a window similar to Figure 43.

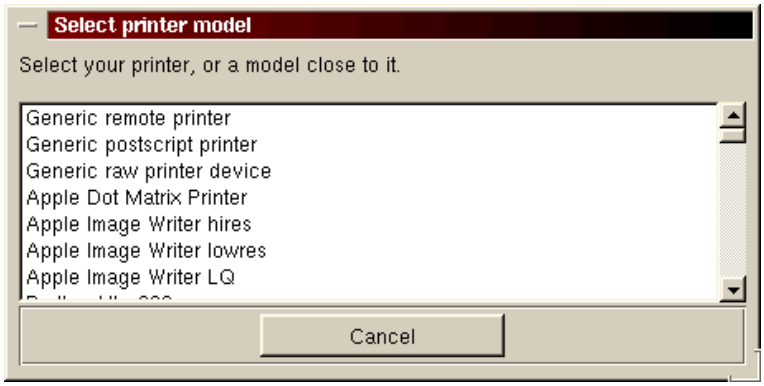


Figure 43. Selecting a printer model

Select your model from the list. After that you will see a window similar to Figure 44.

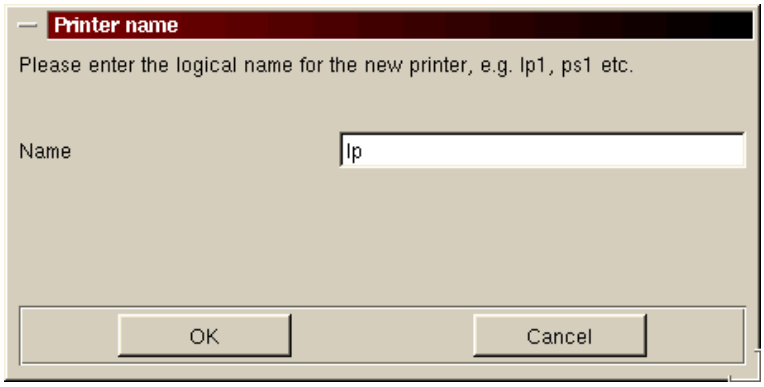


Figure 44. Defining printer logical name

Here you define the logical name of the printer. This name is then used in all printer definitions. Click **OK** to continue, and you will see a window similar to Figure 45.

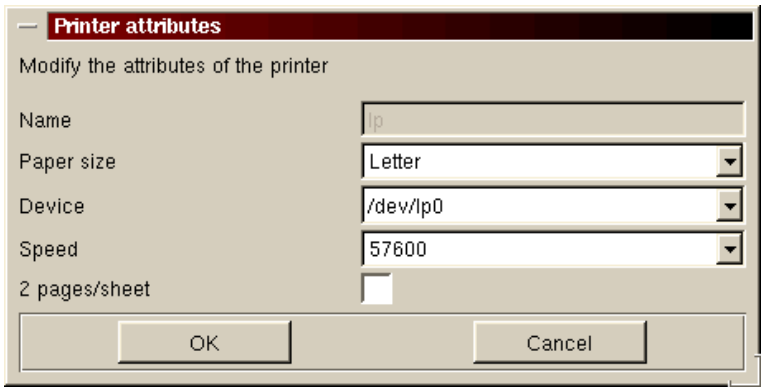


Figure 45. Printer attributes

Here you define printer attributes:

- **Paper size**
- **Device** - this is the physical device to which the printer is connected. This is usually the parallel port, and /dev/lp0 is the first parallel port in your server.
- **Speed** - this is the speed for the data traveling over the device to which the printer is connected.

These attributes are related to the printer driver you choose, so all drivers will not have the same options.

After you have defined all attributes for your printer driver click **OK** to continue. In the next window select **Save** to save your configuration. The installation program will then ask you if it should create the printer queue for your new printer. Click **OK** to create the queue. The printer daemon will be stopped so that the queue can be created and then it will be restarted again.

2.16.2 Removing a printer

You can remove a printer from your system by selecting the printer to be removed from the list of installed printers and select **Printer > Remove**. You will be asked twice if you really want to remove the printer. Answer **OK** both times if you really want to remove the printer.

2.16.3 Edit a printer

If you want to edit the properties of the installed printer, select the printer from the list and choose **Printer > Edit**. You will see a window similar to Figure 46.

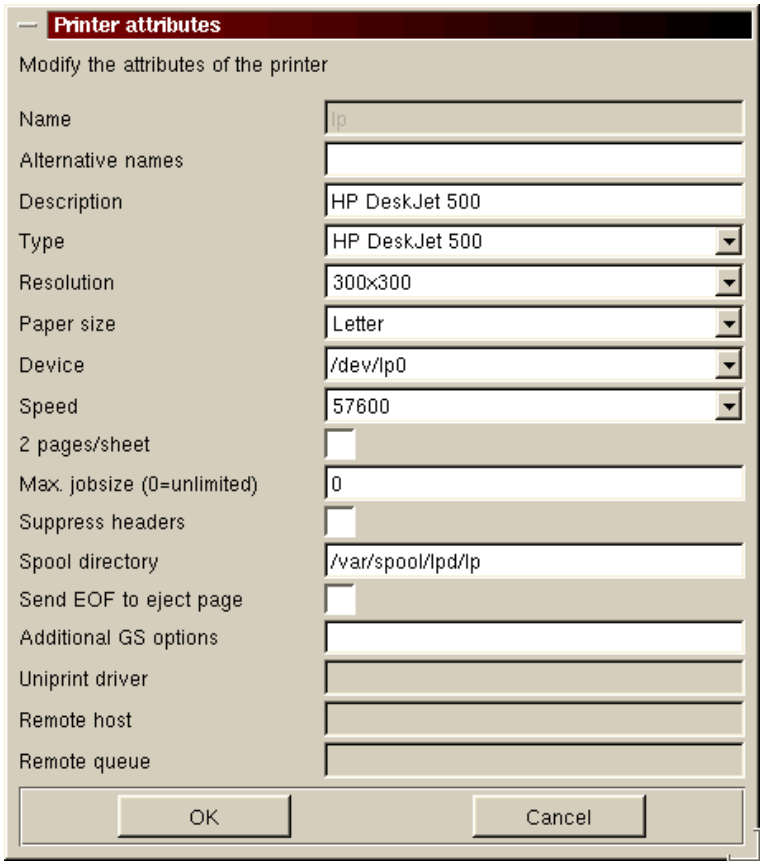


Figure 46. Printer attributes

Edit the preferences you want and click **OK** to continue. In the next window click **Save** to save the changes.

2.17 Network menu

From the Network menu of the COAS tools, you can access the following tools:

- **TCP/IP** - for managing TCP/IP settings.
- **Ethernet interfaces** - for Ethernet Network Interface Cards (NICs).
- **Mail Transfer** - for managing the Mail Transfer Agent (MTA). You can find more information on how to set up MTA on your server in Chapter 9,

"sendmail" of the IBM redbook, *Caldera Openlinux Integration Guide for IBM @server xSeries and Netfinity*, SG24-5861.

The COAS tools menu is shown in Figure 47.

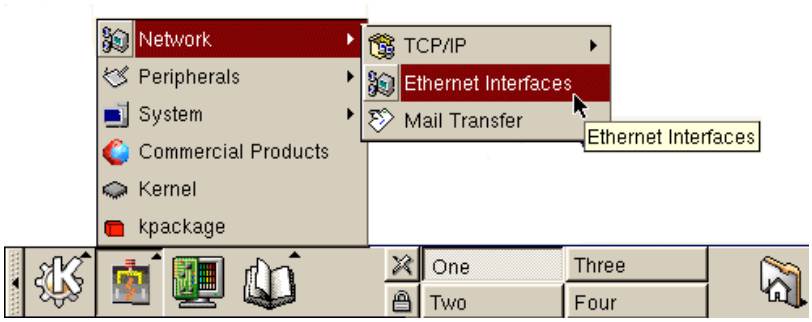


Figure 47. Network menu

To start the tools from the Network menu select the tool you want. At the initial window, click **OK** to continue. If you select **TCP/IP,** you will be presented with two options, as you can see in Figure 48.

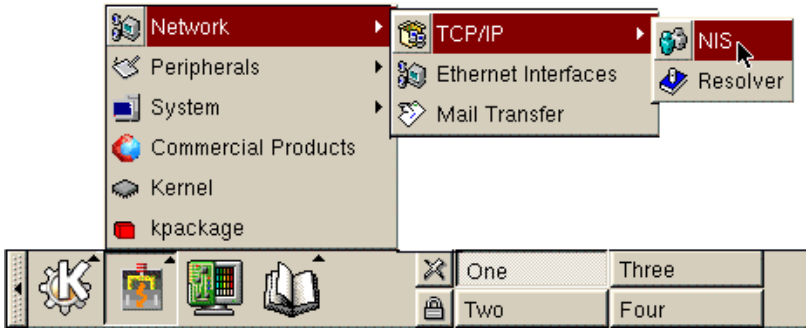


Figure 48. TCP/IP menu

- NIS - for setting the NIS client options. You can get more information on how to set up an NIS client or server in Chapter 11, "NIS - Network Information System" in the IBM redbook, *Caldera Openlinux Integration Guide for IBM @server xSeries and Netfinity*, SG24-5861.
- Resolver - to set up the TCP/IP resolving settings.

2.18 Ethernet interfaces

With this tool you can configure your Ethernet NICs. After you start the tool you will see a window similar to Figure 49.

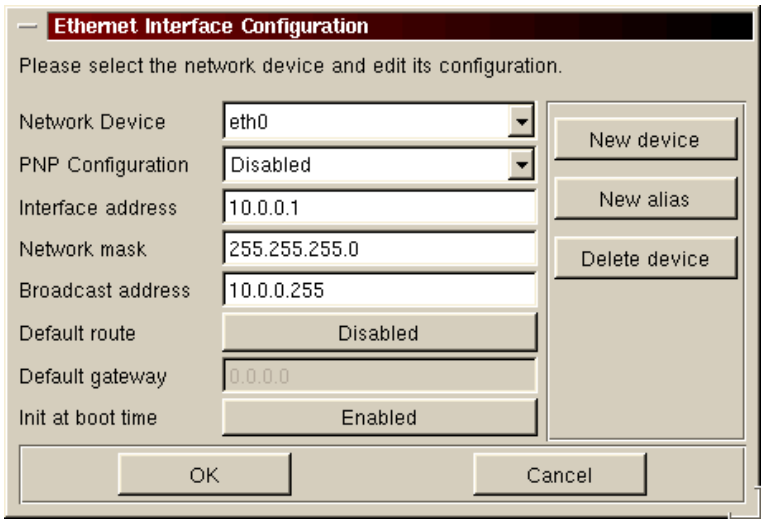


Figure 49. Ethernet Interface Configuration window

If you configured your Ethernet NIC during installation you will see the current configuration. There are several configuration options available:

- Network device - this is the name of the network device as it is recognized by the kernel.
- PNP Configuration - here you can select if the adapter is configured automatically from a DHCP server by selecting the **DHCP** option, or manually by selecting the **Disabled** option.
- Interface address - here you define the IP address of the interface.
- Network mask - here you define the subnet mask for the interface.
- Broadcast address - here you define the broadcast IP address. This is by default calculated from subnet mask.
- Default route - here you enable or disable the default route.
- Default gateway - if you enabled default routing, you need to specify the IP address of the router here.
- Init at boot time - here you specify if the interface should be initialized during system startup.

2.18.1 Adding a new network interface

If you have installed a new Ethernet interface you can add it to the system configuration by clicking **New device.** You will see a window similar to Figure 50.

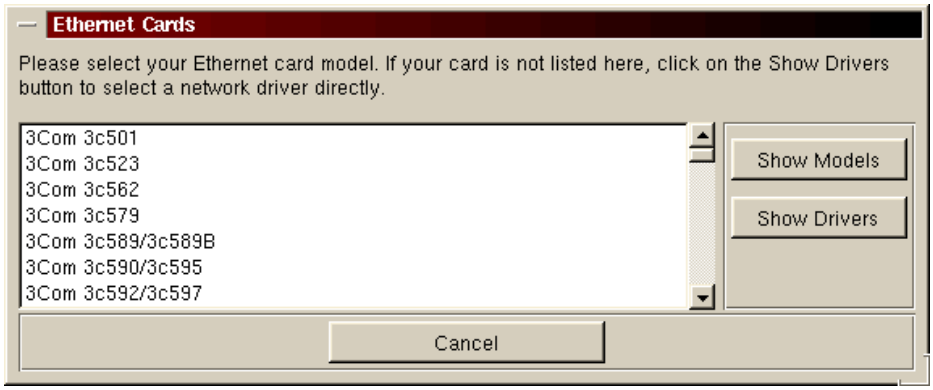


Figure 50. Selecting the type of the Ethernet card

If you do not find the driver for your Ethernet card among the listed models, you may try to check all available drivers. To see all drivers click **Show Drivers.** Select your model/driver by clicking the appropriate one, and you will see a window similar to Figure 51.

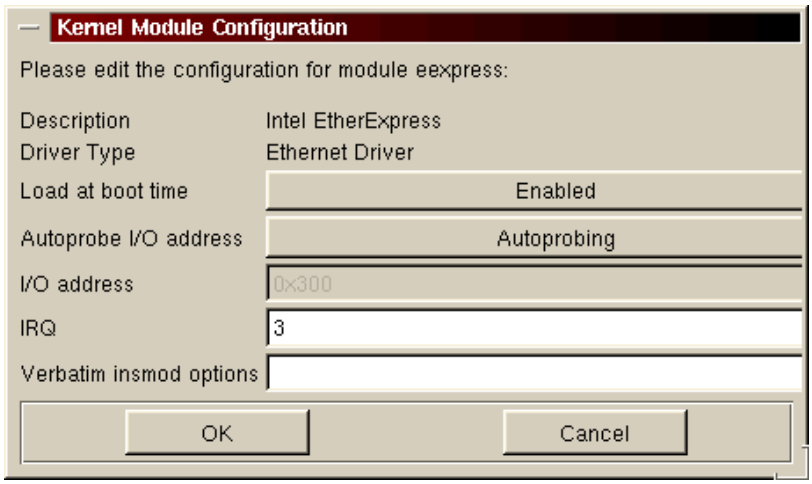


Figure 51. Defining hardware parameters

Here you define the hardware parameters for the driver for your Ethernet NIC. When you are done, click **OK** to continue. The setup utility will try to load the

module you selected. If the loading of the module is successful, your new interface definition will now be available for additional setup. You will see a window similar to Figure 49 on page 42. Define parameters to meet your needs and click **OK** to continue. On the next window click **Save** to save the configuration.

2.18.2 Removing a network interface

If you want to delete the definition for an Ethernet NIC, click **Delete device** from the dialog shown in Figure 49 on page 42. Then click **OK** to close the configuration window. In the next window, click **Save** to save the changes you just made.

If you have more than one Ethernet NIC adapter and you want to remove the adapter eth1 for example, follow these steps:

1. Stop the interface by executing the command:

   ```
   /sbin/ifdown eth1
   ```

2. Delete the file /etc/sysconfig/network-scripts/ifcfg-eth1 by executing the command:

   ```
   rm /etc/sysconfig/network-scripts/ipcfg-eth1
   ```

This procedure can be used for all adapters when you have multiple adapters defined.

2.19 Name resolution settings

You can access the tool for name resolution settings by clicking **Network > TCP/IP > Resolver**. When you start the tool you will see a window similar to Figure 52.

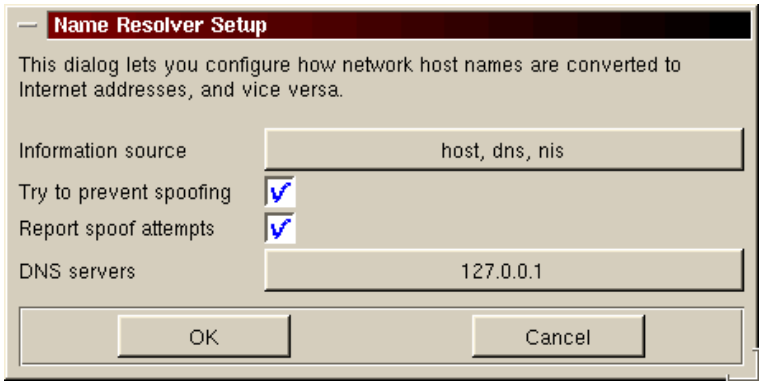


Figure 52. Name resolution setup

Here you can define how the name resolution is performed on your system. You have four options here:

- Information source - here you define the order and sources for the name resolution.
- Try to prevent spoofing
- Report spoof attempts
- DNS servers - the defined IP addresses of the DNS servers

2.19.1 Name resolution order and sources

You can change the name resolution order and sources by clicking the button to the right of **Information sources.** You will see a window similar to Figure 53.

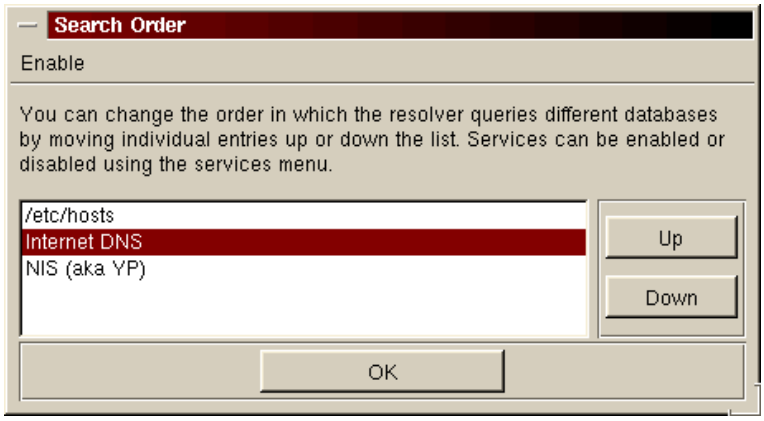


Figure 53. Search order

The search order can be changed by moving the name resolution resources up and down. If you want to enable or disable a particular name resolution source you can do this by selecting **Enable** and selecting the source you want to enable or disable. If a source is currently enabled, you can disable it and vice versa. When you are done, click **OK** to continue and on the next window select **Save** to save the changes.

2.19.2 Defining a DNS server

You can define a DNS server by clicking the button to the right of the **DNS servers** button. You will see a window similar to Figure 54.

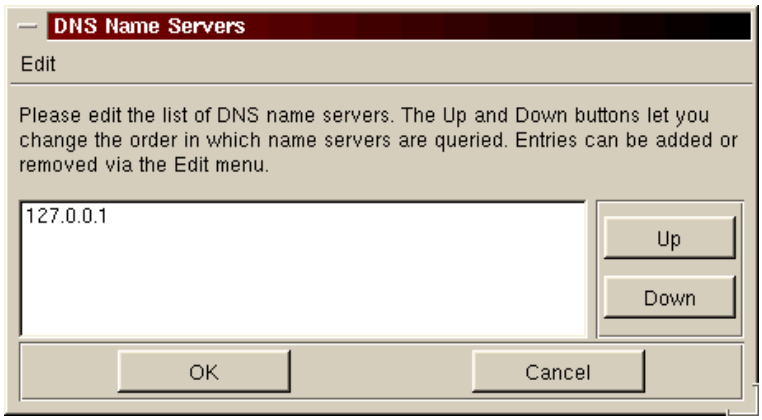


Figure 54. DNS servers

If you have more than one DNS server defined you can reorder them by moving them up and down. The top-most server will be accessed first and so on.

2.19.2.1 Add a new DNS server

If you want to add a new DNS server select **Edit > Add server**. You will see a window similar to Figure 55.

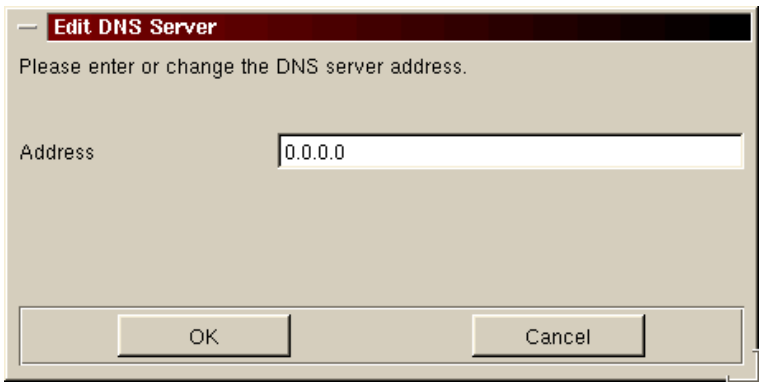


Figure 55. Specifying a DNS server

Type in the IP address of the DNS server and click **OK** to go back to the previous window.

2.19.2.2 Remove a DNS server

If you want to remove a DNS server select it from the list and choose **Edit > Remove server**.

2.19.2.3 Change a DNS server

If you want to change a DNS server's IP address select it from the list and choose **Edit > Edit server**. You will see a window similar to Figure 55. Type in the new IP address of the server and click **OK** to go back to the previous window.

2.20 Manipulating kernel modules

You can manage kernel modules in Caldera OpenLinux by using the kernel configuration tool from the COAS tools. You can start it by selecting **Kernel** from the COAS tools menu. When the Kernel tool is started, you will see a window similar to Figure 56.

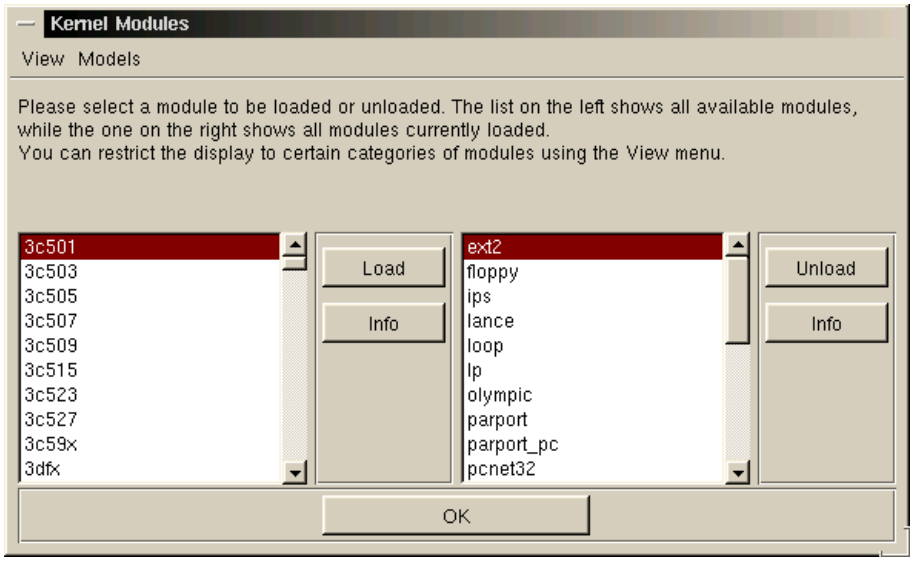


Figure 56. Kernel Modules

On the left side you can see all available modules and on the right side you can see loaded modules. By default all modules are displayed, but if you want to display just one kind of module, you can do this by selecting the following options from the View menu:

- All drivers
- Arcnet drivers
- CD-ROM drivers
- Ethernet drivers
- Misc drivers
- Network drivers
- SCSI drivers
- SCSI host adapter drivers
- Sound drivers
- Token-ring drivers
- ISDN drivers
- Multimedia drivers

If you want to get information about a particular module, select the module from either side and click **Info.**

2.20.1 Loading a new module

When you install a new piece of hardware you need to load the appropriate module if you want the hardware to be useful. In Linux, drivers can be loaded or unloaded without restarting the system. It may take some time to get used to this if you are used to another popular operating system. To load a new module select the module from the left side and click **Load.** You will see a window similar to Figure 57.

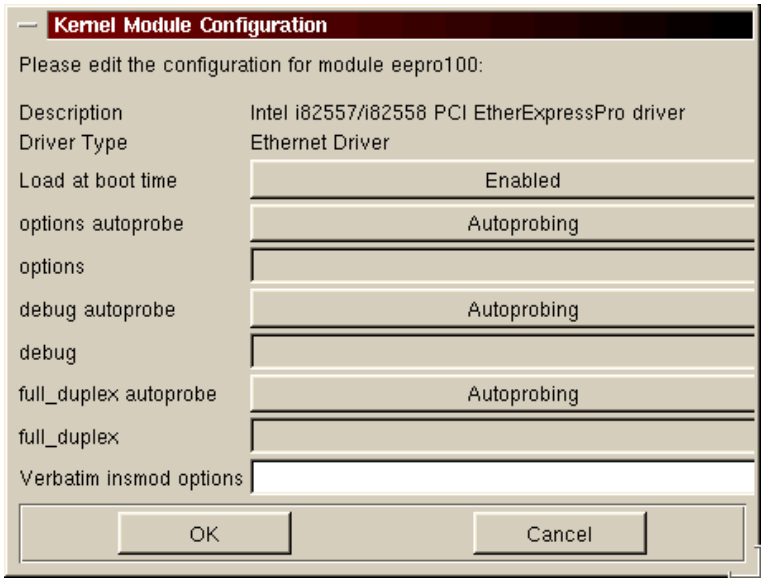


Figure 57. Module configuration

Each module has several hardware-related options and an option to load at boot time. If you want to load a module at boot time, click the button to the right of the Load at boot time field to specify your preferred setting. Click **OK** to actually load the module. If the module is loaded successfully, it will appear on the left side where the loaded modules are displayed.

2.20.2 Unloading a new module

If you want to unload an already loaded module, select it from the left side and click **Unload.** You will be asked if you really want to unload the module. Click **OK** to unload the module. If the module has been enabled to load at system startup, you will see a window similar to Figure 58.

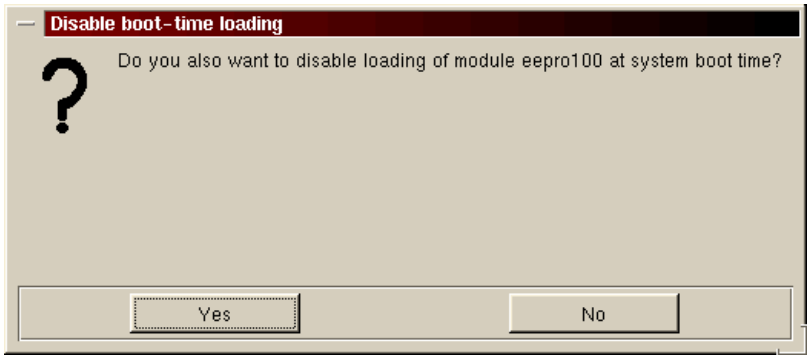


Figure 58. Disabling loading at startup

Here you can decide if you will also disable the startup loading of the module. Select **Yes** or **No** to continue. After that the module will be unloaded.

2.21 Configuring X-Windows

If for whatever reason you need to change the X-Windows setup after installation, you can by executing XF86Setup from the command line.

2.22 System administration using Webmin

In Caldera OpenLinux eServer 2.3, you can also perform administration with the Webmin tool. This is a Web-based interface for managing. Webmin is basically an HTTP daemon acting as an interface to the system files.

More information on Webmin can be obtained from the IBM redbook, *Caldera OpenLinux Integration Guide for IBM @server xSeries and Netfinity*, SG24-5861-01. This redbook can be downloaded in PDF format from the following Web site:

```
http://www.redbooks.ibm.com
```

Chapter 3. Red Hat Linux basic system administration

There are certain commands and procedures that you will need in order to maintain your Linux system. In this chapter we cover basic command-line administration and an introduction to the graphic or menu-driven tool called Linuxconf.

3.1 Finding Linux commands

When you wish to run a program or use a command from the command-line prompt, you may not know where they are located in the directory structure. You can run most of these commands or programs without needing to know where they are because your search path includes a number of directories that will be searched whenever you try to execute a command or run a program. The search path is given by the environment variable $PATH. If you want to find out where a command is located, execute the command:

```
whereis command_name
```

Where `command_name` is the command you are looking for. For example, if you want to find the command `adduser`, execute:

```
whereis adduser
```

You notice that this command is located in the /usr/sbin directory. Many of the major administrative commands will be found in the /usr/sbin directory.

3.2 Package management using RPM

Package management can be done directly with the Red Hat package manager (RPM) on the command line. You can do this either from a straight Linux command-line prompt, or you can do this from an X-Windows generated by one of the window managers.

The following table shows some of the most frequently used versions of the `rpm` commands.

Table 3. Basic RPM commands

Command	Description
`rpm -q <package>`	If package is installed, check version and build number of installed package
`rpm -qi <package>`	Obtain some more information about an installed package

© Copyright IBM Corp. 2001

Command	Description
`rpm -qa`	List all installed packages
`rpm -qf <filename>`	Determine the (installed) package that `<filename>` belongs to
`rpm -Uhv <package.rpm>`	Update/install the file `package.rpm` showing a progress bar
`rpm -F -v ./*.rpm`	Update (freshen) all currently installed packages using the RPM files in the current directory
rpm --help	Get help about the different options and parameters

More information and options about RPM can be found in the manual page (man rpm), and in the RPM how-to at `http://www.rpm.org`. You can also display a short overview by running `rpm --help`.

3.3 User administration

Linux is a multi-user operating system. To differentiate between the various users, each user has to log in with a unique user name and password. Each user belongs to a primary user group, but he can also be a member of other groups as well (up to 16 groups). Each user name is associated with a user ID (UID), which is also unique throughout the system. The same applies to user group names and group IDs (GIDs).

Usually each user has a personal home directory. This is space on the file system (usually a directory below /home, for example /home/username) which belongs to him and where he can store his personal files (for example, e-mail or text documents). Other users generally have no access to the files stored therein.

It is one of the root user's tasks to add and remove user or group accounts. To do this from a menu you can use the program Linuxconf to add, modify or delete groups or users. In the next section we will provide details about user administration from the command prompt.

You should carefully consider adding user groups before adding users. Sometimes there are concerns about restricting access to some parts of the user filesystem. You can do this by creating separate user groups to control access to various files and file systems. Also if you are going to be creating a system with many users, you should consider creating separate groups

divided by what they are doing on the system. You can create an admin group for administrators, a db2user group for DB2 users, and so forth. Linux allows you to control access to both files and directories by both users, groups, and everyone on the system.

Another concern in setting up users and groups is that you may want to share files with other systems. This can be done by the CD, tape, diskette or any similar device. You can use the network to share information with NFS, Samba, IPX and other network packages. If you use user and group names and characteristics that are not the same on all systems doing the sharing, then you can have file sharing and access problems.

If you are creating logins and groups on each system separately, it is often best to use a single system where all your IDs can be created. This system is then used as a reference. It is not necessary that everyone actually log into the reference system. It only exists to coordinate ID and group creation and to prevent non-standard IDs and groups. A user also cannot log into the reference system if the password is not enabled. This will prevent unauthorized access to the system. Red Hat Linux will automatically create a new group for each new user unless you tell it not to.

You might also consider network-wide user authentication and tracking schemes such as NIS, NIS+ and various other network administration packages.

3.3.1 Adding users

To add users to the Linux system you can use the command `useradd` or `adduser`. In Linux you can find the options to `useradd` by typing the command by itself as shown in Figure 59. This is recommended only for commands that you know require an option. Otherwise, you may inadvertently execute a command you do not want to.

```
# useradd
usage: useradd [-u uid [-o]] [-g group] [-G group,...]
                [-d home] [-s shell] [-c comment] [-m [-k template]]
                [-f inactive] [-e expire mm/dd/yy] [-p passwd] [-n] [-r] name
       useradd -D [-g group] [-b base] [-s shell] [-f inactive] [-e expire mm/d
d/yy]
#
```

Figure 59. The useradd command

You can also use the `man` command as shown in Figure 60. You actually see the first window of several windows of information.

```
]# man useradd

USERADD(8)                                                USERADD(8)

NAME
       useradd - Create a new user or update default new user
       information

SYNOPSIS
       useradd [-c comment] [-d home_dir]
               [-e expire_date] [-f inactive_time]
               [-g initial_group] [-G group[,...]]
               [-m [-k skeleton_dir] | -M] [-s shell]
               [-u uid [-o]] [-n] [-r] login

       useradd -D [-g default_group] [-b default_home]
               [-f default_inactive] [-e default_expire_date]
               [-s default_shell]

DESCRIPTION
   Creating New Users
       When invoked without the -D option, the useradd command
       creates a new user account using the values specified on
:
```

Figure 60. Using the man useradd command

Other commands have information presented by using the `--help` option. This option is not implemented in all commands, but in the case of the `useradd` command it will present basically the same information you see in Figure 59.

You can find out what your current default values are with the command `useradd -D` as shown in Figure 61.

```
# useradd -D
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
#
```

Figure 61. Default values for creating a user ID

The explanation of the options shown in Figure 60 are as follows:

`-c comment`

This is a comment field about the user. It has been traditionally called the GECOS field and can include such information as office room numbers,

phone numbers, etc. Any string of characters must be put into double quotes. For example, `-c comment "John Doe, rm. 45, x 78965"`.

`-d home_dir`

The home directory location of the user. If this is not specified then the default is to append the login name to the end of the default value for HOME shown in Figure 61. For example, the home directory for jdoe will be /home/jdoe unless specified here.

`-e expire_date`

This is the date on which the user account will be disabled. The date is specified in the format MM/DD/YY where MM is the month, DD is the date and YY is the two-digit format of the year. (Note that even though the date is represented in two digits, Linux converts the date to a format that is not Y2K dependent, so there are no Y2K worries here.) The default is the value of EXPIRE in Figure 61.

`-f inactive_time`

This gives the status of the account. The value of 0 says to disable the account when the password expires. A value of -1 says not to disable it. The default is the value of INACTIVE in Figure 61.

`-g initial_group`

The initial group that a user logs in with. This can be a name or number of a currently existing group. This is specified in the /etc/password file as the GID or Group ID value. The default group is given by the value of GROUP in Figure 61.

`-G group[,...]`

This is a list of any additional existing groups the user may belong to. Each group is separated by a comma.

`-m [-k skeleton_dir] | -M`

The `-m` option says to create the user's home directory if it does not exist. The `skeleton_dir` is the location of files that are copied to a new user's directory. The default location, if you do not use the `-m` option, is the `/etc/skel` directory. The default is the value of SKEL in Figure 61.

`-s shell`

The is the shell that the user will first log in with. The default is the value of SHELL in Figure 61.

`-u uid [-o]`

This is the numeric UID or user ID number that is used by Linux to distinguish one user from the other. All UIDs must be unique unless the `-o` option is used. The `-o` option is often used for creating IDs that have the same access rights, but different logins and passwords. The system looks only at the UID and GID values for determining access rights.

`-n`

By default a group will be created whose GID is the same as the UID of the user being created. The `-n` option will turn off this Red Hat originated behavior.

`-r`

This is used to create a system account whose UID is lower than a certain number defined in /etc/login.defs. You will also need to specify the `-m` option if you want to create the home directory. Otherwise, it will not be created. System accounts generally have UID values between 0 and 99.

`login`

This is the login name that the user will log in with. This will need to be unique on the system.

3.3.2 Modifying users

You can modify user logins with the `usermod` command:

```
[root@redhat /root]# usermod
usage: usermod [-u uid [-o]] [-g group] [-G group,...]
               [-d home [-m]] [-s shell] [-c comment] [-l new_name]
               [-f inactive] [-e expire mm/dd/yy] [-p passwd] name
[root@redhat /root]#
```

Figure 62. The usermod command

The options for the `usermod` command are basically the same as those for the `useradd` command, so they will not be repeated except for those that are different. With the `usermod` command you need to observe the following options:

`-d home [-m]`

The `-m` option says to move the contents of the current home directory to the new home directory and create the directory if it does not exist.

`-l new_name`

This allows you to change the users' user names that they log in with. A user cannot be logged in with this name when you do this.

`-p passwd`

This allows you to set the password of the user from the command line. This can be useful if you have a program that automates password creation, since you can use a variable in the place of the `passwd` string.

```
USERMOD(8)                                                USERMOD(8)

NAME
       usermod - Modify a user account

SYNOPSIS
       usermod [-c comment] [-d home_dir [-m]]
               [-e expire_date] [-f inactive_time]
               [-g initial_group] [-G group[,...]]
               [-l login_name] [-s shell]
               [-u uid [-o]] login

DESCRIPTION
       The usermod command modifies the system account files to
       reflect the changes that are specified on the command
       line. The options which apply to the usermod command are

       -c comment
              The new value of the user's password file comment
              field. It is normally modified using the chfn(1)
              utility.
:
```

Figure 63. Results of the man usermod command

3.3.3 Deleting users

The command to delete users is `userdel`. You can see the options in Figure 64. This command is a lot simpler because there is not much choice you have when deleting a user.

```
[root@redhat /root]# userdel
usage: userdel [-r] name
[root@redhat /root]#
```

Figure 64. The userdel command

The results of `man userdel` are seen in Figure 65.

```
USERDEL(8)                                                USERDEL(8)

NAME
       userdel - Delete a user account and related files

SYNOPSIS
       userdel [-r] login

DESCRIPTION
       The userdel command modifies the system account files,
       deleting all entries that refer to login. The named user
       must exist.

       -r     Files in the user's home directory will be removed
              along with the home directory itself.    Files
              located in other file system will have to be
              searched for and deleted manually.

FILES
       /etc/passwd - user account information
       /etc/shadow - secure user account information
:
.
```

Figure 65. Man userdel command

The only option that you can use is:

```
-r
```

This says for you to remove the home directory and its contents. Otherwise the home directory and its contents will not be deleted.

3.3.4 File system permissions

Linux has inherent security features, the most visible being filesystem permissions. Setting permissions on files allows the system administrator to restrict access to parts of the file system.

File permissions can be set on files and directories. The easiest way to see an example of this is looking in the /home directory:\

```
mail:/home # ls -l
total 1
drwxr-xr-x  19 root     root          396 Nov 15 21:06 .
drwxr-xr-x  22 root     root          467 Nov 13 16:28 ..
drwx------   6 davej    users         912 Nov 15 21:05 davej
drwx------   6 george   users         912 Nov 15 21:03 george
drwx------   6 ivo      users         912 Nov 15 21:02 ivo
drwx------   6 jakob    users         912 Nov 15 21:03 jakob
drwx------   6 jasmin   users         912 Nov 15 21:04 jasmin
drwx------   6 jens     users         912 Nov 15 21:04 jens
drwx------   6 jhaskins users         912 Nov 15 21:02 jhaskins
drwx------   6 justin   users         912 Nov 15 21:06 justin
drwx------   6 lenz     users         912 Nov 15 21:03 lenz
drwx------   6 linux    users         912 Nov 15 21:03 linux
drwx------   6 malcom   users         912 Nov 15 21:04 malcom
drwx------   6 rachael  users         912 Nov 15 21:03 rachael
drwx------   6 rafiu    users         912 Nov 15 21:04 rafiu
drwx------   6 ruediger users         912 Nov 15 21:04 ruediger
drwx------   6 rufus    users         912 Nov 15 21:02 rufus
drwx------   6 ted      users         912 Nov 15 21:03 ted
drwx------   6 uzi      users         912 Nov 15 21:04 uzi
mail:/home #
```

Figure 66. Viewing file permissions

Taking the usr linux as an example:

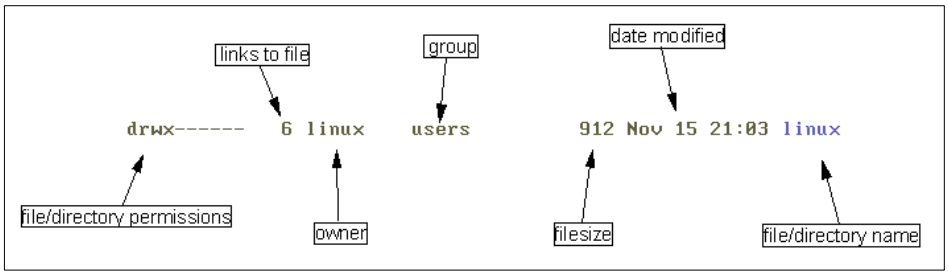


Figure 67. Explanation of ls output

What we are most interested in is the file/firectory permissions. This signifies a lot of information in a short amount of space:

d - The first character in the permissions signifies this is a directory.

l - a symbolic link to another file.

- - a normal file.

c - refers to files in the /dev direcotry. This signifies the file represents a character device.

b - refers to files in the /dev directory. This signifies the file represents a block device.

rwx - In this case it allows only the owner of the file (in this case linux) to read, write and execute this file.

Type	Owner	Group	World
d	rwx	---	---

As you can see, the format of the string is becoming a bit easier to read.

The owner of the file is the user that created the file. The group part is the group that owns the file (for example, the group users). The world part means everyone else. Setting a permission in the world part sets the permission for every user, irrelevant of their group membership and so on.

Here is another example:

```
-rwxr-xr--
```

This means that this is a normal file, the owner can read, write and execute the file, the group can read and execute the file, and everyone else can read the file, but not modify or execute it.

As for directories, if you set a directory as:

```
drwxrw-rw-
```

you are saying that only the directory owner is allowed to execute something “inside” the directory. So if another user tries to change directory (cd) into this directory, they will get a “permission denied” error message. This is excatly what happens with regards to users’ home directories.

To change the permissions on a file, you use the `chmod` command. Only root can modify files that do not belong to them. you must own the file to be able to change its permissions.

The easiest way to change permissions is to use symbolic representations of what you want permissions to be.

```
chmod g+rw myfile
```

This is one of the simplest ways of changing a permission. You are saying that you want the file `myfile` to allow all members of the **g**roup to be able to read and write to it.

If you used a **-** (minus sign) instead of a plus, you would be taking away thos permissions. This would mean that members of the group would not be allowed to read or write to the file.

You can mix adding and removinf permissions in the same command:

```
chmod u+x-rw myfile
```

This will allow executing the file, but will not allow reading or writing the file for the file owner.

Here is a summary of the symbolic representatoins available in the `chmod` command:

r - read

w - write

x - execute

- - take away the permissions

+ - add the permissions

s - set the SUID bit. This says that if the file is executable, it will be run as the owner of the file, not as the user that is running the file.

3.4 Setting up your hardware

To set up your hardware from the command line, you need to be aware of what devices you have on your system. Knowing your hardware and how to set it up will pay off later in the time saved.

3.4.1 Determining your hardware

There are several ways you can do this. These methods include:

- Bootup messages: The system will attempt to find hardware devices when you boot up. It may recognize the hardware devices and then attempt to use modules that are compiled in the kernel or modules that are loaded separately. Sometimes the system will recognize the hardware but will be unable to load the modules due to some hardware or setup inconsistencies or version dependencies.
- `dmesg`: This is a command that you can run anytime and will display many of the messages that you see on bootup.

- Mail - Linux can mail you a copy of the configuration and bootup messages for every reboot. This can be more extensive than the messages from `dmesg`. To get access to these messages, type `mail`.
- Other tools: There are public domain utilities such as Lothar that you can use to determine your hardware characteristics.

An understanding of the hardware configuration is very important because Linux allows you to have a lot more control over your system than many other operating systems. It also allows you to fix problems more quickly because information is not hidden.

You can also determine what hardware the system has found by looking in the file system /proc. This file system is not really a directory at all but a window into memory. This does have files and directories, but they are not saved onto the disk. It shows you what the system thinks exists in terms of hardware. You can see the contents of this file system in Figure 68. You will also see the contents of one of the listings in the file system. In this case it is the interrupts file, which shows the interrupts that appear to be used. There are several other files and directories located here that have useful information.

```
[root@redhat /proc]# ls
1    278  330  444  545  564  bus          kmsg     net         tty
192  286  331  445  546  565  cmdline      ksyms    parport     uptime
2    3    344  446  547  566  cpuinfo      loadavg  partitions  version
200  306  354  447  548  585  devices      locks    pci
211  314  365  450  549  586  dma          mca      rtc
219  324  4    451  551  587  filesystems  mdstat   scsi
229  325  421  466  554  599  fs           meminfo  self
237  326  431  467  556  6    ide          misc     slabinfo
247  327  441  470  558  600  interrupts   modules  stat
257  328  442  5    559  744  ioports      mounts   swaps
268  329  443  527  561  89   kcore        mtrr     sys
#
# cat interrupts
           CPU0
  0:    1060623          XT-PIC  timer
  1:        451          XT-PIC  keyboard
  2:          0          XT-PIC  cascade
  8:          1          XT-PIC  rtc
  9:       3236          XT-PIC  PCnet/PCI II 79C970A
 12:       1209          XT-PIC  PS/2 Mouse
 13:          0          XT-PIC  fpu
 14:     201594          XT-PIC  ide0
 15:         29          XT-PIC  ide1
NMI:          0
#
```

Figure 68. The contents of the /proc directory and the interrupts file

3.4.2 Loading in your hardware modules

You can determine what modules are loaded with the command `lsmod` as in Figure 69. This will list the modules that have been loaded. It is actually the same as the /proc/modules file that is listed in Figure 68.

```
# lsmod
Module                  Size  Used by
nfsd                  141104   8  (autoclean)
nfs                    27924   1  (autoclean)
lockd                  29132   1  (autoclean) [nfsd nfs]
sunrpc                 48700   1  (autoclean) [nfsd nfs lockd]
pcnet32                 9064   1  (autoclean)
iBCS                  115616   0
parport_probe           2940   0  (autoclean) (unused)
lp                      4960   0  (unused)
parport                 6676   0  [parport_probe lp]
vfat                    9092   0  (unused)
#
```

Figure 69. The lsmod command

If you need to add a module, you can determine the module name by going to the directory /lib/modules as you see in Figure 70.

```
[root@redhat /etc]# cd /lib/modules
[root@redhat modules]# ls
2.2.16-22
[root@redhat modules]# cd 2.2.16-22
[root@redhat 2.2.16-22]# ls
block  cdrom  fs  ipv4  ipv6  misc  modules.dep  net  pcmcia  scsi  uusbd
[root@redhat 2.2.16-22]# ls net
3c501.o       com20020.o  es3210.o        ne2k-pci.o     slhc.o
3c503.o       com90io.o   eth16i.o        ne3210.o       slip.o
3c505.o       com90xx.o   ewrk3.o         ni5010.o       smc-mca.o
3c507.o       cops.o      fmv18x.o        ni52.o         smc-ultra.o
3c509.o       cosa.o      hostess_sv11.o  ni65.o         smc-ultra32.o
3c515.o       cs89x0.o    hp-plus.o       olympic.o      smc9194.o
3c523.o       de4x5.o     hp.o            pcnet32.o      strip.o
3c527.o       de600.o     hp100.o         plip.o         syncppp.o
3c59x.o       de620.o     ibmtr.o         ppp.o          tlan.o
82596.o       depca.o     ipddp.o         ppp_deflate.o  tulip.o
8390.o        dgrs.o      ircomm.o        rcpci.o        via-rhine.o
ac3200.o      dlci.o      irda.o          rtl8139.o      wanpipe.o
acenic.o      dummy.o     irlan.o         sb1000.o       wavelan.o
arc-rimi.o    e2100.o     lance.o         sdla.o         wd.o
arcnet.o      eepro.o     lapbether.o     sdladrv.o      x25_asy.o
arlan-proc.o  eepro100.o  lne390.o        sealevel.o     yellowfin.o
arlan.o       eexpress.o  ltpc.o          shaper.o       z85230.o
at1700.o      epic100.o   ne.o            sk_mca.o
bsd_comp.o    eql.o       ne2.o           sktr.o
[root@redhat 2.2.16-22]#
```

Figure 70. Finding loadable hardware modules

The next place that you need to look is the file /etc/modules.conf. This file contains the list of modules that you will load when you boot the system. It contains aliases, such as eth0, that are linked to the names of actual modules that are loaded. It also contains options that you might need to load to make certain hardware work in Linux. When you want a module to be included on the bootup sequence you can add it to this file. For example, to add an IBM ISA token-ring device on bootup, create the entry:

```
alias tr0 ibmtr
```

Add the above line in the /etc/modules.conf file and the module will be loaded on bootup.

```
# cat /etc/modules.conf
alias eth0 pcnet32
alias eth0 pcnet32
alias net-pf-6 off
alias char-major-14 sb
options sb io=0x220 irq=5 dma=1 dma16=5 mpu_io=0x330
#
```

Figure 71. /etc/modules.conf file

3.4.3 Setting up your network cards

You first need to verify whether Linux recognized your network hardware. You can look at the resources listed in 3.4.1, “Determining your hardware” on page 61. If you do not see it listed, you need to verify that the hardware is set up properly. You can go to the manuals that came with the hardware or see if the manufacturer has other information available. Then you need to see if the hardware is supported. To select the supported entries to get the hardware compatibility list for your current version of Red Hat Linux, go to:

```
http://www.redhat.com
```

You can determine which network cards have modules loaded by looking at Figure 69 on page 63. If you do not see the modules for your network card, you need to manually load the module or modules with the following command:

```
insmod module_name
```

Where the module_name is selected from those in Figure 70. If you do not see the module for your specific hardware device then you can do some research on the Internet. Besides `http://www.redhat.com`, you should try the Web site for the manufacturer of the hardware you are using. Many manufacturers are making it a point to include support for Linux.

Once the module is successfully loaded, you can add it to the /etc/modules.conf file as discussed earlier and it will be loaded on bootup.

Once you have all modules loaded, either automatically or manually, you need to determine that networking is in place. To see all of the network devices that have been recognized and have had their modules loaded, type the command:

```
ifconfig
```

If this is a new device for TCP/IP you may find that some items such as the inet address need to be defined.

```
# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:81:6A:1A
          inet addr:172.16.1.234  Bcast:172.16.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3665 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1192 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:9 Base address:0x1000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:3924  Metric:1
          RX packets:642 errors:0 dropped:0 overruns:0 frame:0
          TX packets:642 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
#
```

Figure 72. The ifconfig command

You can manually set up the TCP/IP addressing by using the `ifconfig` command. Let us say we found a device called eth0 and we want to use the command line to set up networking. Use the command:

`ifconfig eth0 address` **`new_address`** `netmask` **`new_netmask`**

Where:

`new_address` is the new IP address that is to be assigned to the network devices. An example is `172.16.1.234` .

`new_netmask` is the new netmask that is to be assigned to this. An example is `255.255.255.0` .

Now execute the `ifconfig` command again to verify that your settings are enabled.

The next step is to establish any routing that you need to do. You do this with the `route` command. The generic format of this command is:

`route add -net` **`network_address network_dev`**

Where:

`network_address` is the address of the network you want to access. This usually has all 0's in the network address positions where the netmask has 255. In other words, a netmask of 255.255.255.0 when applied to an address of 172.16.1.222 will give a network address of 172.16.1.0.

network_dev is the name of the Network Interface Card that was either assigned by the system or you assigned to it in /etc/modules.conf. An example would be eth1.

So an example of setting up the routing on an Ethernet card on eth1 would be:

```
route add -net 172.16.1.0 eth1
```

This says that you can get to network 172.16.1.0 by going through eth1.

Note

If you replace those network address related 0's with 255 in the above example, you will get the broadcast address, which in the example above makes the broadcast address 172.16.1.255.

The actual network configurations are stored in the directory /etc/sysconfig/network-scripts. Each interface has a separate file. For eth0, this file is called ifcfg-eth0. You can see a sample file in Figure 73. There will be one for each interface that you have on your system.

The following values are set up in this file:

DEVICE: This is the alias device that you set up in /etc/modules.conf.

IPADDR: This is the IP address that is assigned to the Network Interface Card.

NETMASK: This is the netmask discussed earlier.

NETWORK: This is the network address.

BROADCAST: This is the broadcast address.

ONBOOT: Start up the device on bootup.

BOOTPROTO: This is any boot prototype file that might be used.

```
# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
IPADDR=172.16.1.234
NETMASK=255.255.255.0
NETWORK=172.16.1.0
BROADCAST=172.16.1.255
ONBOOT=yes
BOOTPROTO=none
#
```

Figure 73. ifcfg-eth0 file

Once all your system configuration files are set up you should have a working network. You should reboot your network to verify that the system is loading the files properly on bootup.

3.4.4 Enabling remote services to your server

In order to enable certain types of remote access to your system, Linux may require some additional configuration to be done.

The /etc/services file lists which kind of services you are going to make available on which ports. A partial listing of the file is shown in Figure 74. You will notice that each service is assigned a number. This is the port number. You will note that FTP is assigned 21, and telnet is assigned 23.

```
#partial listing of /etc/services
#
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
msp             18/tcp                          # message send protocol
msp             18/udp                          # message send protocol
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp             21/tcp
fsp             21/udp          fspd
ssh             22/tcp                          # SSH Remote Login Protocol
ssh             22/udp                          # SSH Remote Login Protocol
telnet          23/tcp
# 24 - private
smtp            25/tcp          mail
# 26 - unassigned
time            37/tcp          timserver
time            37/udp          timserver
rlp             39/udp          resource        # resource location
nameserver      42/tcp          name            # IEN 116
{The remainder of file is not displayed}
```

Figure 74. /etc/services file partial listing

However, you cannot do a telnet or any type of remote access into a system unless the service is activated. This is controlled by files in the /etc/xinetd.d/ directory.

```
#
[root@test1 xinetd.d]# cat telnet
# default: on
# description: The telnet server serves telnet sessions; it uses \
#       unencrypted username/password pairs for authentication.
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
}

[root@test1 xinetd.d]#
```

Figure 75. The /etc/xinetd.d/telnet file

Verify the service file is in the /etc/xinetd directory. If it is not, you can create it.

Now we need to edit the /etc/hosts.allow and/etc/hosts.deny files.

In the /etc/hosts.allow file, which is shown in Figure 76, you see that the only host that is allowed is the localhost, which is 127.0.0.1. This means you can do a telnet localhost or telnet 127.0.0.1 and that is all unless access is prevented by the hosts.deny file.

```
# hosts.allow   This file describes the names of the hosts which are
#               allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
#
# See man hosts_access(5) for more information

ALL : 127.0.0.1
```

Figure 76. The /etc/hosts.allow file

In order to add additional remote access to your server, you need to add an additional line. If you want to allow access to all other hosts then add the line:

```
ALL : ALL
```

This will enable your remote access.

You also need to edit the /etc/hosts.deny file. This file is seen in Figure 77. You will notice that access is denied to all remote systems. This will also prevent access from the localhost entry even though it is specified in the /etc/hosts.allow file.

```
#
# hosts.deny    This file describes the names of the hosts which are
#               *not* allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
#
# See man hosts_access(5) for more information.

ALL: ALL
```

Figure 77. /etc/hosts.deny

In order to allow access from all remote hosts you need to remove or comment out the last line in Figure 77:

```
# ALL: ALL
```

This will then allow access to all remote hosts.

Note

When making changes to configuration files it is a good habit to copy the original file to a backup file. You can do something like:

```
cp file_name file_name.bak
```

(where `file_name` is the file you are using)

Put a comment symbol, generally the #, in front of any entries you want to change. Then create a new line with the revised information. This allow you to return to your previous entries in case of errors and you can go totally back to your original file if it is copied.

Then you need to restart the inetd daemon with the following command:

```
killall -HUP xinetd
```

You can test that your telnet is working with the following command:

`telnet your_ip` (where `your_ip` is the IP address of your system)

If you can log in successfully, then you know that the remote access is working.

3.5 A brief introduction to Linuxconf

Linuxconf is a utility that allows you to configure and control various aspects of your system. In this section we will give a brief overview of Linuxconf's capabilities. If you would like to find out more about Linuxconf, the project Web site is:

```
http://www.solucorp.qc.ca/linuxconf/
```

3.5.1 Starting Linuxconf

In order to use Linuxconf, you must be logged in as root. It is advised that administrators log in as themselves and `su` to root. For more information on the `su` command, type: `man su`.

Linuxconf has several user interfaces:

- Command-line
- Menu-driven
- X-Windows
- Web-based

The default interfaces are menu driven and X-Windows. Which interface you actually use is decided by your display environment variable.

Regardless of which interface you are using, Linuxconf has a tree format. You can collapse or expand a tree by selecting the parent. Selecting the lowest level of a tree will bring up a new menu for configuring options.

3.5.2 Running Linuxconf

For the purpose of this chapter we will be using the X-Windows interface; however all are essentially the same utility. To start Linuxconf from X-windows, type:

```
linuxconf
```

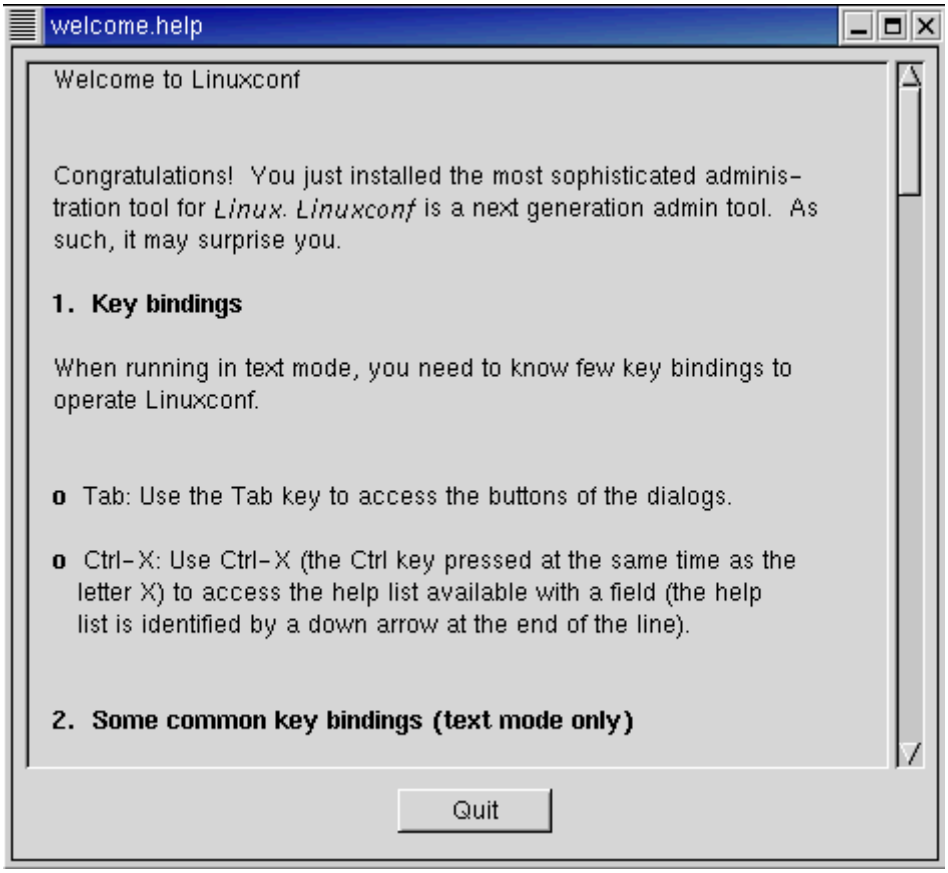


Figure 78. Linuxconf initial startup

The first time you run Linuxconf you are presented with a welcome window that provides tips for using Linuxconf.

Click **Quit** to continue to the Linuxconf interface.

3.5.3 What can I do with Linuxconf?

Linuxconf's greatest strength is the incredible range of configuration options under its control. The following is a brief but by no means complete list of options:

- Networking options:
  - Basic host information: Set host and domain names. You can set up multiple network interfaces, assigning IP addresses and specifying drivers.

- DNS usage: Set the default domain, multiple name servers and search domains.
- Routing and Gateways: Set a default gateway and routes to other networks.
- Set options for NIS, NFS, a DHCP server, an Apache Web server, SMB, FTP, IPX interfaces, and PPP information.

- User Accounts administration (Figure 79):

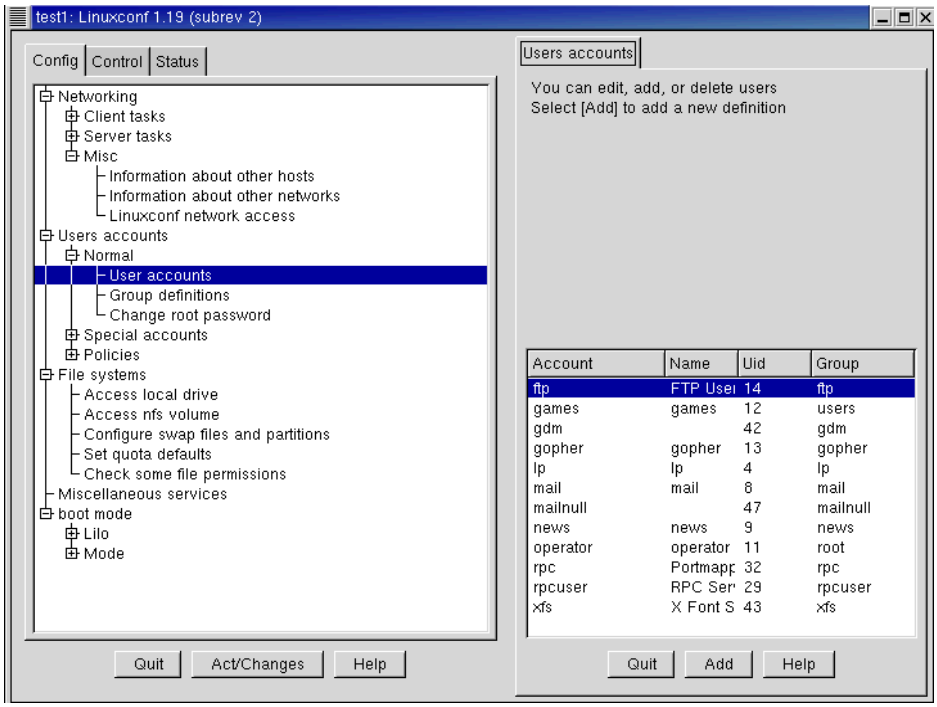


Figure 79. User Account options

You can do basic and some advanced user administration including adding, deleting, or modifying user accounts. You can set options for password management, schedule job definitions, configure mail settings, and define group definitions.

- File systems:

  You can control mount points, swap files, partitions, NFS volumes, quotas, and some file permissions.

- Miscellaneous Services:

  You can specify initial system services and a modem port.

- Boot mode:

  Basic LILO configuration including options for booting new kernels and setting your boot level (3 for text mode or 5 for Graphic).

- Control Options (Figure 80):

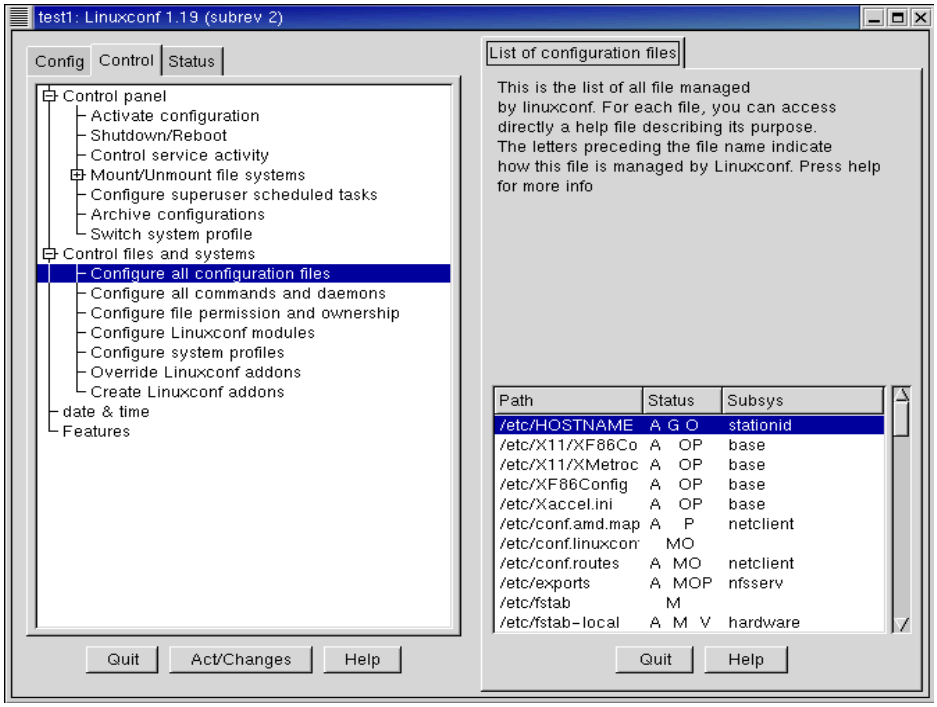


Figure 80. Control options

Control allows you to activate the current Linuxconf configuration, shut down, reboot, control basic services installed, mount and unmount file systems, schedule superuser tasks, and many other crucial configuration options.

3.5.4 Enabling a service to start on bootup automatically

Enabling a service to start on bootup is a common procedure. In this example we have installed Samba and would like the service to start automatically. To do this we will use the Linuxconf utility. In this example we will be using the

X-Windows version of Linuxconf; however all versions of Linuxconf are essentially the same. To start Linuxconf from an X-Windows terminal, type:

```
linuxconf
```

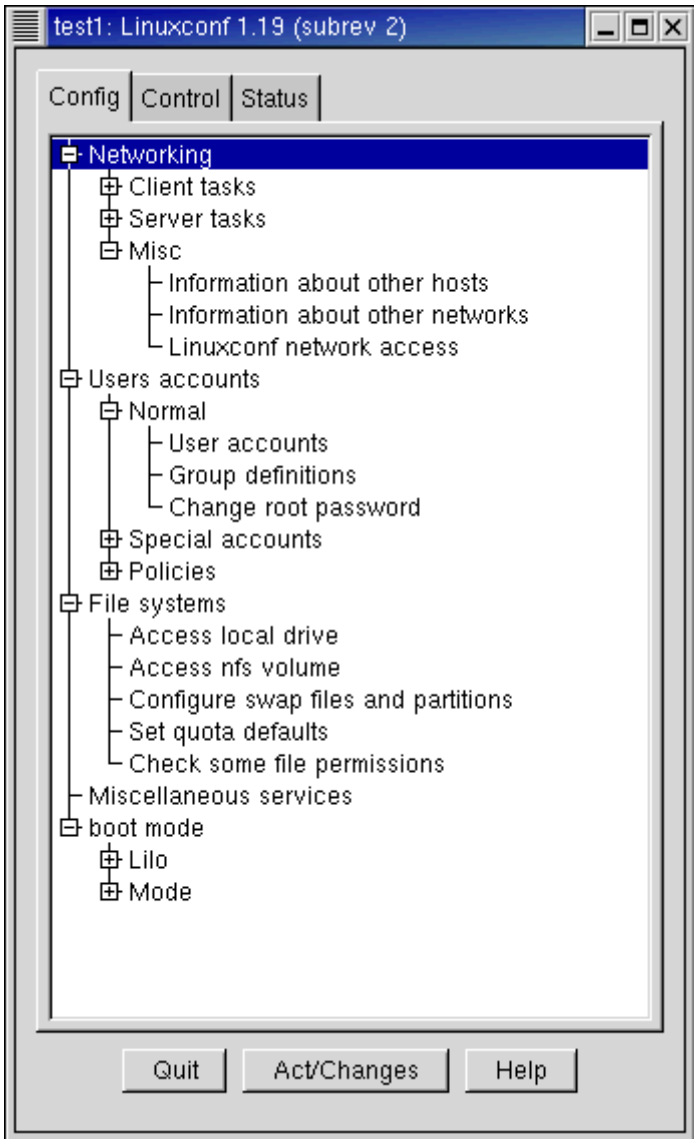


Figure 81. Starting Linuxconf

This launches the Linuxconf utility (see Figure 81). Click the **Control** tab and select **Control Services Activity.** See Figure 82.

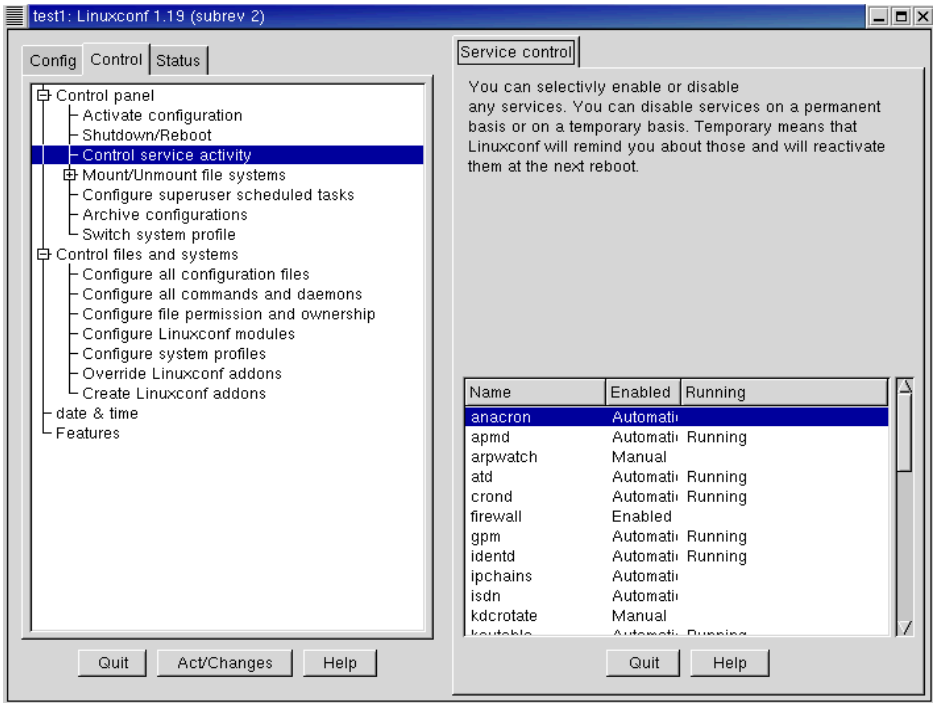


Figure 82. Selecting control service activity

In the service control window, all the services we have installed on our Linux system are visible. In this example we are using Samba, the smb service. Scroll down and select the **smb** service.

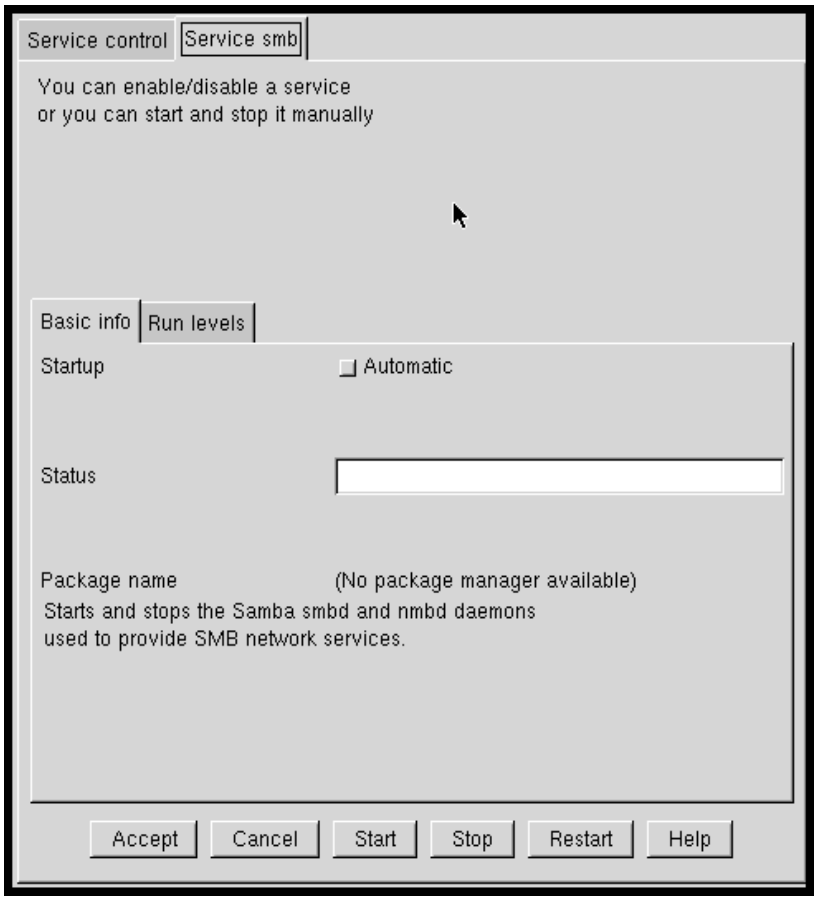


Figure 83. Enabling the service to start up automatically at boot

Click the **Startup Automatic** box. We also have the options of starting, stopping, or restarting the service.

Click the **Accept** button.

Verify that the smb service is enabled (for automatic startup) and quit Linuxconf. When the Linux server reboots, the Samba services will automatically be started.

3.6 Summary

This concludes our basic administration section. For more information on running Linux take a look at the Linux Documentation project Web site:

http://www.linuxdoc.org

or read *Running Linux* by Matt Welsh, published by O'Reilly.

Chapter 4. SuSE Linux basic system administration

This chapter will give you an overview of how to perform the most common administrative tasks on a SuSE Linux system. Most of these tasks can be done with YaST, SuSE's configuration and administration tool. However, you may still edit the different configuration files manually, if you wish. YaST will detect manual changes and will not overwrite them.

4.1 Adding and removing software packages using YaST

SuSE Linux uses the RPM package manager to manage software packages of the distribution. RPM uses a database to store information about all files that belong to a certain package, including some additional information about the package. RPM itself is a command-line program. You can use it from the command line to add, remove or obtain information about software packages and system files. See 4.2, "Package management using RPM" on page 85 for more details. YaST, SuSE's administration and configuration tool, can act as a user-friendly front end to RPM.

To install or remove software packages, insert the first CD-ROM and start SuSE's installation and configuration tool YaST by typing `yast` at the command line (as user root). YaST will start up and you will see YaST's main menu.

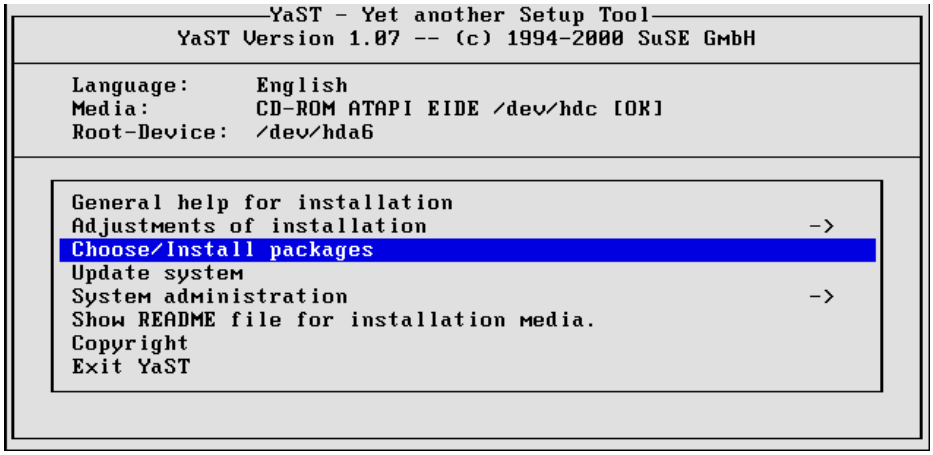


Figure 84. YaST: main menu

Highlight the menu entry **Choose/Install packages** and press Enter. Alternatively, you can invoke YaST with the following parameters:

© Copyright IBM Corp. 2001

```
yast --mask install --autoexit
```

This will automatically open the installation main menu and will return to the command line on exit.

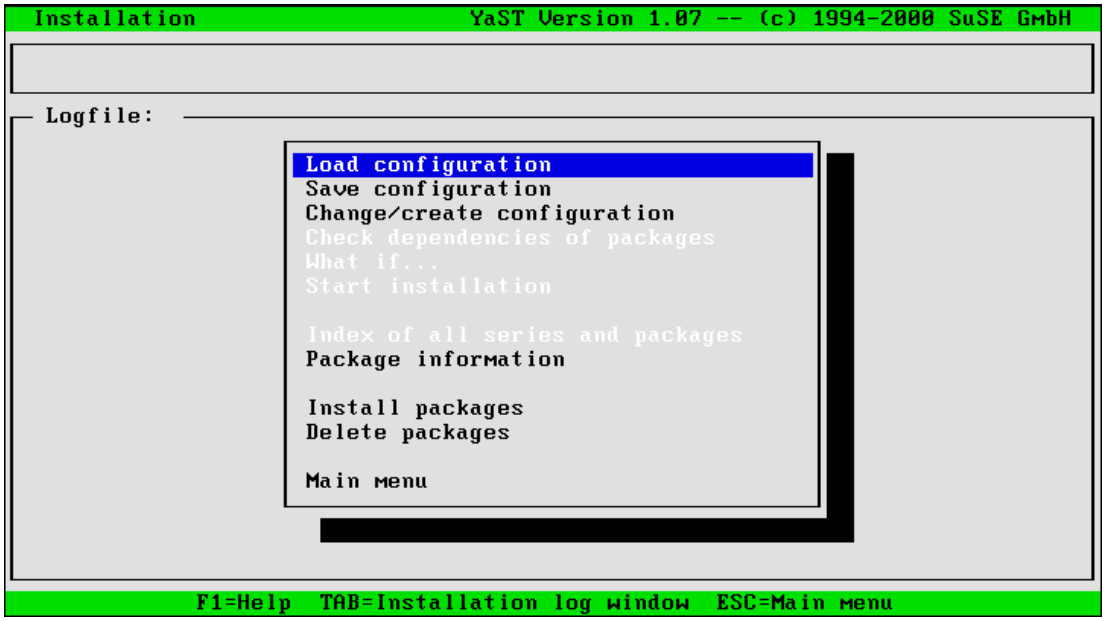


Figure 85. YaST: package installation main menu

SuSE Linux offers a choice of software configurations. These contain a list of selected software packages to fit a certain need. Select **Load configuration** to load a predefined configuration.

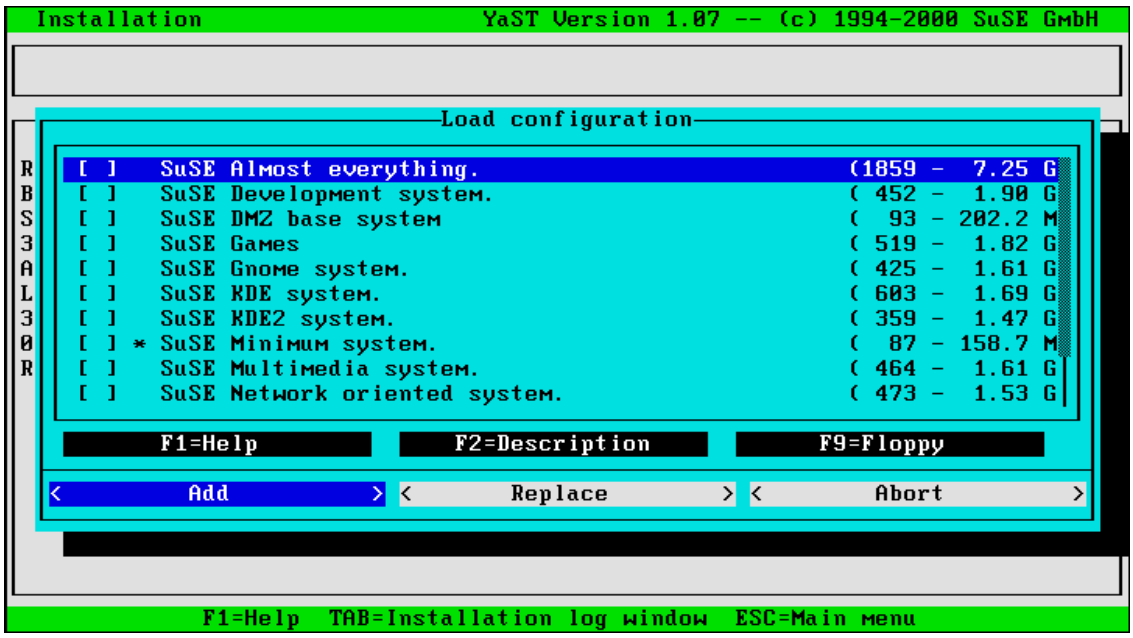


Figure 86. YaST: load software configuration

You can now add the files from a configuration to your current configuration, or you can replace it with one of these configurations. If you replace a configuration, all currently installed packages that are not part of the selected configuration will be marked for deletion! Press Esc to return to the main menu.

To add packages to or remove packages from your current configuration, select **Change / create configuration**. This will open the Series selection window shown in Figure 87.

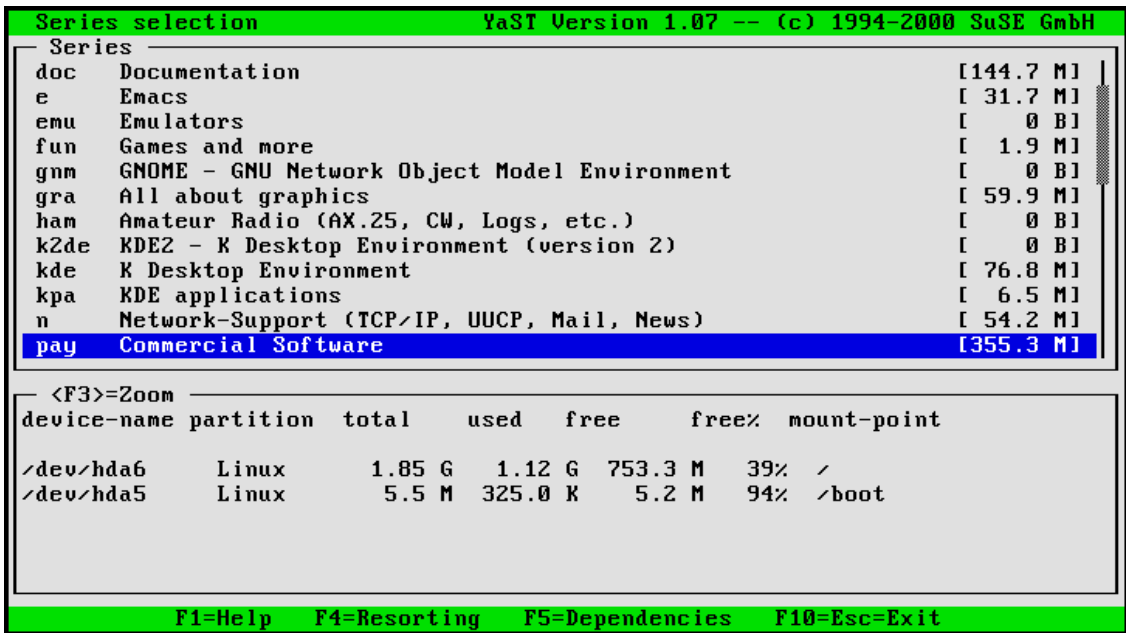


Figure 87. YaST: series selection

All software packages are categorized into different series. Choose your category and press Enter to see all packages belonging to this series.

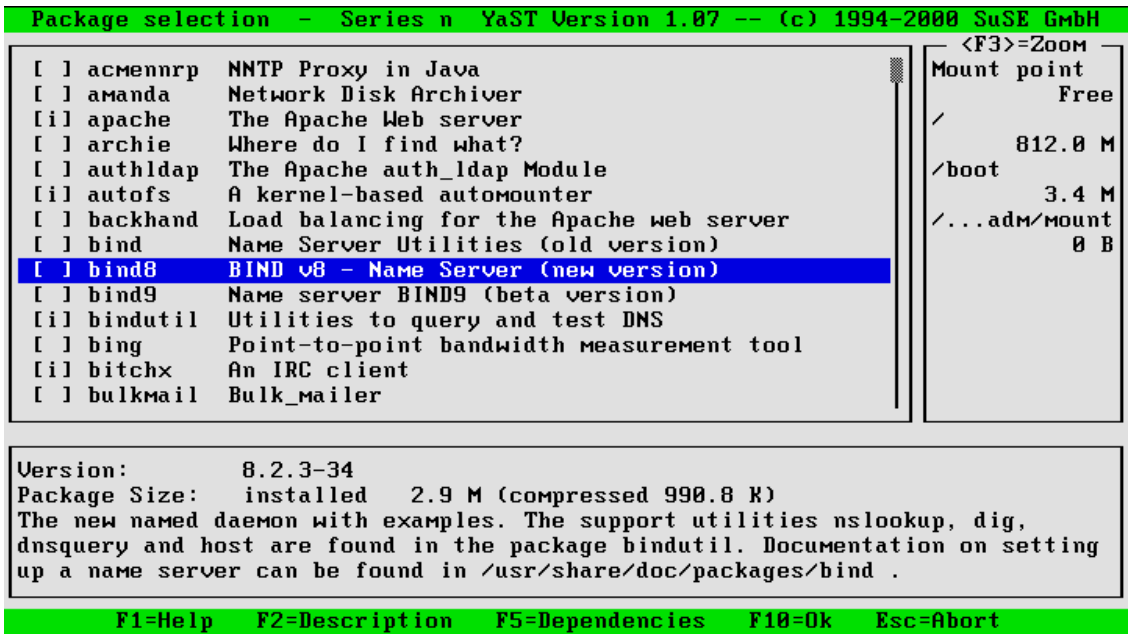


Figure 88. YaST: package selection

To select a package for installation/removal/update, press the Spacebar or Enter. This will toggle the status of the selected package. The indicator in the first column displays the current status:

Table 4. Package selection indicators

Indicator	Package status
[ ]	Package is not installed and not selected for installation
[X]	Package is marked for installation
[i]	Package is already installed
[R]	Package is installed and will be replaced / reinstalled
[D]	Package is installed and marked for deletion

If you want to change the package status of multiple packages at once, press Shift+A (see Figure 89).

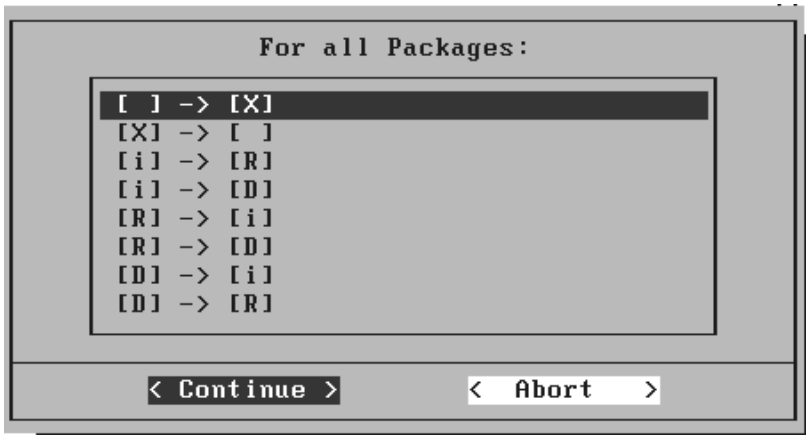


Figure 89. YaST: apply changes to all packages

After you have made your choice, press F10 to return to the series selection. You can now select or remove packages from other series, or press F10 once more to return to the software configuration main menu. If you made any modifications to your current software configuration, you can start the actual installation or removal of packages by selecting **Start Installation**. If you want to verify what packages will be installed, removed or replaced, select **What if...**

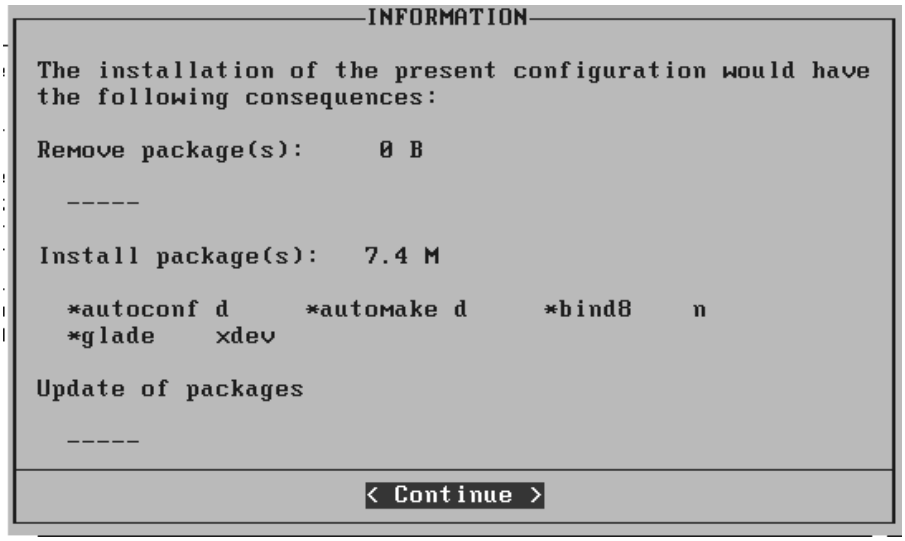


Figure 90. YaST: what if...

Click **Continue** to return to the main menu. If you are satisfied with your selection, select **Start installation**. YaST will now check on which CD the necessary packages are located and will prompt you for the respective CD. After the packages have been installed, you will return to the main menu shown in Figure 85 on page 80. You can now either add or remove additional packages. If you want to save your current package selection (for example for copying it to another system), select **Save configuration**.You will then be prompted where you want to save the configuration to. Select **to floppy** or **to hard disk**, depending on your needs. If you are saving to a floppy disk, make sure that it does not contain valuable data! The diskette will be erased during this process.

You can return to the YaST main menu by selecting **Main menu**.

4.2 Package management using RPM

Package management can also be done directly with the Red Hat package manager (RPM) on the command line. The following table shows some of the most frequently used commands.

Table 5. Basic RPM commands

Command	Description
`rpm -q <package>`	If package is installed, check version and build number of installed package
`rpm -qi <package>`	Obtain some more information about an installed package
`rpm -qa`	List all installed packages
`rpm -qf <filename>`	Determine the (installed) package that <filename> belongs to
`rpm -Uhv <package.rpm>`	Update/Install the file package.rpm showing a progress bar
`rpm -F -v ./*.rpm`	Update (freshen) all currently installed packages using the RPM files in the current directory
`rpm --help`	Get some help about the different options and parameters

Note

If you install packages using RPM on the command line, make sure to run the script SuSEconfig afterwards! Some packages require post-installation maintenance.

More information and options about RPM can be found in the manual page (man rpm), the RPM how-to

`(less /usr/share/doc/howto/en/RPM-HOWTO.txt.gz)`

and on the RPM Web site at `http://www.rpm.org`. You can also display a short overview by running

`rpm --help`.

4.3 User and group administration using YaST

Linux is a multi-user operating system. To differentiate between the various users, each user has to log in with a unique user name and password. Each user belongs to a primary user group, but they can also be a member of other groups as well (up to 16 groups). Each user name is associated with a user ID (UID), which is also unique throughout the system. The same applies to user group names and group IDs (GIDs).

Usually each user has a personal home directory. This is space on the file system (usually a directory below /home, for example /home/username) that belongs to a person and where the person can store their personal files (for example e-mail or text documents). Other users generally have no access to the files stored in another user's home directory.

You should carefully consider adding user groups before adding users. Sometimes there are concerns about restricting access to some parts of the user file system. You can do this by creating separate user groups to control access to various files and filesystems. Also if you are going to be creating a system with many users, you should consider creating separate groups divided by what they are doing on the system. You can create an admin group for admins, a db2user group for DB2 users, and so forth. Linux allows you to control access to both files and directories by users, groups, and everyone on the system.

Another concern in setting up users and groups is that you may want to share files with other systems. This can be done by CD-ROM, tape, diskette or any similar device. You can use the network to share information with NFS,

Samba, IPX and other network packages. If you use user and group names and characteristics that are not the same on all systems doing the sharing, then you can have file sharing and access problems.

If you are creating logins and groups on each box separately, it is often best to use a single system where all your IDs can be created. This system is then used as a reference. It is not necessary that everyone actually log into the reference system. It only exists to coordinate ID and group creation and to prevent non-standard IDs and groups. A user also cannot log into the reference system if the password is not enabled. This will prevent unauthorized access to the system. If you want to administer a lot of users on different machines, you should consider setting up NIS. See Chapter 12, “NIS -Network Information System” or Chapter 13, “LDAP - Lightweight Directory Access Protocol” in the IBM redbook, *SuSE Linux Integration Guide for IBM @server xSeries and Netfinity*, SG24-5863 for more information about this.

It is one of the root user’s tasks to add and remove user or group accounts. With YaST, SuSE provides an easy-to-use tool for user and group administration. To use it, log in as the root user and type the command:

```
yast --mask user --autoexit
```

Alternatively you can invoke YaST by simply typing `yast` and choosing **System administration -> User administration**. The following window will appear:

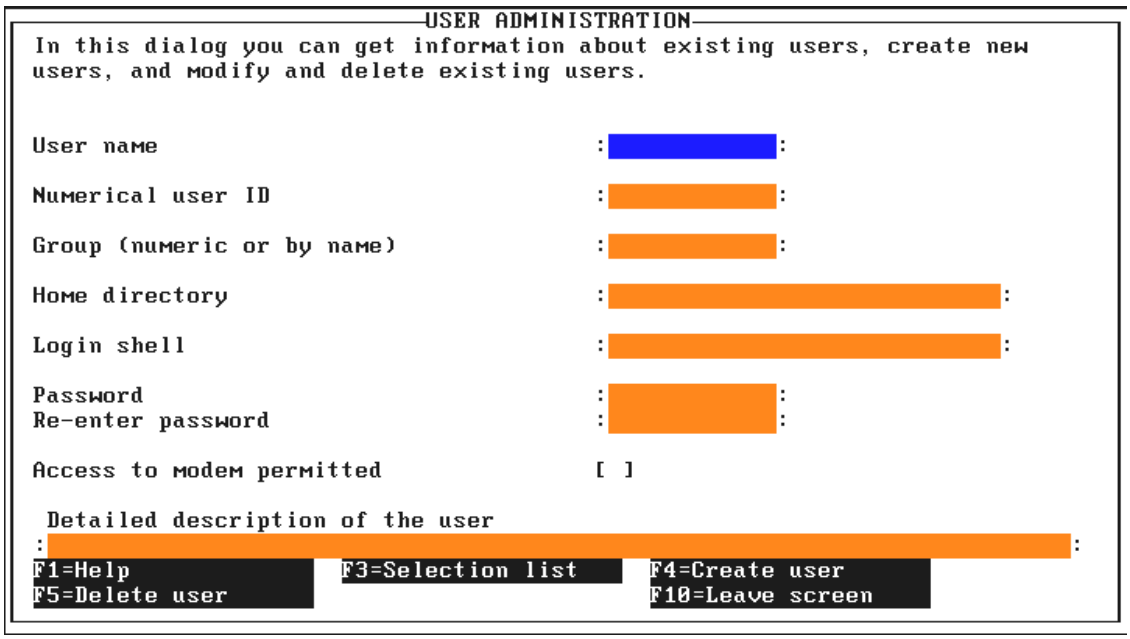


Figure 91. YaST: user administration main window

To add a new user, fill in the blanks. The user name should be short and in lowercase (YaST will do some verification on the input). After you pressed Tab or Enter to advance to the next input field, YaST will automatically look for the next available user ID and will assign it to this user. The entries Group, Home directory and Login shell will also be filled with default values, but you are free to change them to fit your requirements.

Some information about the different shells:

- **/bin/bash** - This is the Bourne Again Shell, which is an extension to the Bourne Shell. This is the most popular shell for Linux.
- **/bin/sh** - This is the standard Bourne Shell that has been around since almost the beginning of UNIX.
- **/bin/ash** - This is another version of the Bourne Shell.
- **/bin/bsh** - This is the same as /bin/ash to which it is linked.
- **/bin/ksh** - This is the standard Korn shell that is the most popular shell for UNIX Administration.
- **/bin/tcsh** - This is a public domain extension of the C Shell.

- **/bin/csh** - This is the standard C Shell that originated at the University of California, Berkeley.
- **/bin/zsh** - This is another extension of the Bourne Shell.

Your choice of shells is a matter of preference, but generally UNIX admins prefer Bourne or Korn Shell programs, whereas programmers tend to prefer C Shell-based programs.

If you want this user to be able to connect to the Internet using a modem, check **Access to modem permitted**. This will add this user to the user groups dialout and uucp, which have the necessary permissions to initiate a dial-up connection using the tool wvdial. The entry fields User name, Group and Login shell also provide a selection list where you can choose a previously defined value. Press F3 in the respective entry field.

After you have filled in all fields, press F4 to actually create the user. If the home directory of that user did not exist before, it will now be created and the contents of the directory /etc/skel will be copied into it. This skeleton directory contains a basic framework of configuration files for the user to start from.

If you want to remove a user account, just select the login name using F3 or enter the name manually in the user name input form. To delete this user, press F5 and confirm the following question with **Yes.** You will be prompted for a confirmation before the user's home directory will be removed, too.

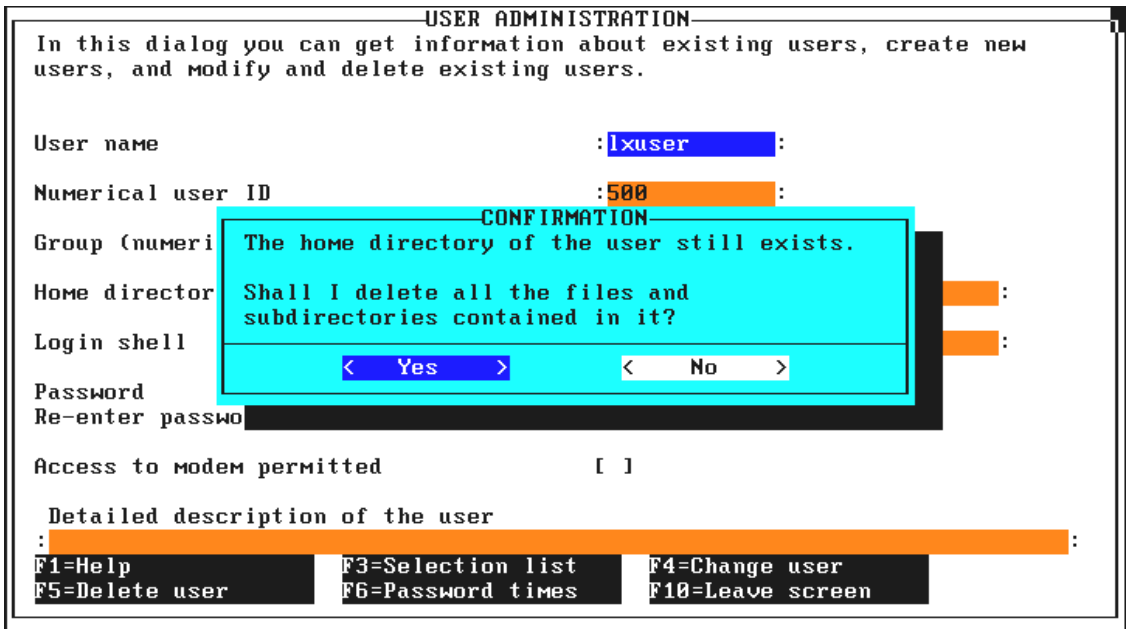


Figure 92. YaST: home directory removal confirmation

After you have finished the user administration, press F10 to return to the main menu.

4.4 Adding users on the command line

To add users to the Linux system you can also use the command `useradd`. In Linux you can find the options to `useradd` by typing the command by itself as in Figure 93. This is recommended only for commands that you know require an option. Otherwise, you may inadvertently execute a command you do not want to.

```
SuSE:~ # useradd
usage: useradd  [-u uid [-o]] [-g group]  [-G group,...]
                [-d home]  [-s shell]  [-c comment]  [-m [-k template]]
                [-f inactive]  [-e expire ]  [-p passwd]  name
       useradd  -D [-g group]  [-b base]  [-s shell]
                [-f inactive]  [-e expire ]
```

Figure 93. The useradd command

You can also use the `man` command to obtain more detailed information about the different parameters.

Other commands have information presented by using the `--help` option. This option is not implemented in all commands but in the case of the `useradd` command it will present basically the same information you see in Figure 93.

You can find out what your current default values are with the command `useradd -D` as shown in Figure 94.

```
SuSE:~ # useradd -D
GROUP=100
HOME=/home
INACTIVE=0
EXPIRE=10000
SHELL=/bin/bash
SKEL=/etc/skel
```

Figure 94. Default values for creating a user ID

The explanation of the options are as follows:

`-c comment`

This is a comment field about the user. It has been traditionally called the General Electric Comprehensive Operating System (GECOS) field and can include such information as office room numbers, phone numbers, etc. Any string of characters must be put into double quotes. For example, `-c comment "John Doe, rm. 45, x 78965"`.

`-d home_dir`

The home directory location of the user. If this is not specified then the default is to append the login name to the end of the default value for HOME shown in Figure 94. For example, the home directory for jdoe will be /home/jdoe unless specified here.

`-e expire_date`

This is the date on which the user account will be disabled. The date is specified in the format MM/DD/YY where MM is the month, DD is the date and YY is the two-digit format of the year. (Note that even though the date is represented in two digits, Linux converts the date to a format that is not Y2K dependent, so there are no Y2K worries here.) The default is the value of EXPIRE in Figure 94.

`-f inactive_time`

This gives the status of the account. The value of 0 says to disable the account when the password expires. A value of -1 says not to disable it. The default is the value of INACTIVE in Figure 94.

`-g initial_group`

The initial group that a user logs in with. This can be a name or number of a currently existing group. This is specified in the /etc/password file as the GID or Group ID value. The default group is given by the value of GROUP in Figure 94.

`-G group[,...]`

This is a list of any additional existing groups the user may belong to. Each group is separated by a comma.

`-m [-k skeleton_dir]`

The `-m` option says to create the user's home directory if it does not exist. The `skeleton_dir` is the location of files that are copied to a new user's directory. The default location, if you do not use the `-m` option, is the `/etc/skel` directory. The default is the value of SKEL in Figure 94.

`-s shell`

The is the shell that the user will first log in with. The default is the value of SHELL in Figure 94.

`-u uid [-o]`

This is the numeric UID or user ID number that is used by Linux to distinguish one user from the other. All UIDs must be unique unless the `-o` option is used. The `-o` option is often used for creating IDs that have the same access rights, but different logins and passwords. The system looks only at the UID and GID values for determining access rights.

`-r`

This is used to create a system account whose UID is lower than a certain number defined in /etc/login.defs. You will also need to specify the `-m` option if you want to create the home directory. Otherwise, it will not be created. System accounts generally have UID values between 0 and 99.

`login`

This is the login name that the user will log in with. This will need to be unique on the system.

4.4.1 Modifying users - the command line version

You can modify user logins with the `usermod` command.

```
# usermod
usage: usermod [-u uid [-o]] [-g group] [-G group,...]
               [-d home [-m]] [-s shell] [-c comment] [-l new_name]
               [-f inactive] [-e expire ] [-p passwd] name
```

Figure 95. The usermod command

The options for the `usermod` command are basically the same as those for the `useradd` command, so they will not be repeated except for those that are different. With the `usermod` command you need to observe the following options.

`-d home [-m]`

The `-m` option says to move the contents of the current home directory to the new home directory and create the directory if it does not exist.

`-l new_name`

This allows you to change the user's user name that he logs in with. The user cannot be logged in with this name when he does this.

`-p passwd`

This allows you to set the password of the user from the command line. This can be useful if you have a program that automates password creation, since you can use a variable in the place of the passwd string.

4.4.2 Deleting users - the command line version

The command to delete users is `userdel`. You can see the options in Figure 96. This command is a lot simpler because there is not much choice you have when deleting a user.

```
# userdel
usage: userdel [-r] name
```

Figure 96. The userdel command

The only option that you can use is:

`-r`

This says for you to remove the home directory and its contents. Otherwise, the home directory and its contents will not be deleted.

4.4.3 Group administration using YaST

To administer user groups, select **System Administration -> Group administration** from the YaST main menu. Alternatively, start YaST from the command line using the following parameters:

```
yast --mask group --autoexit
```

This will get you directly to the group administration window:

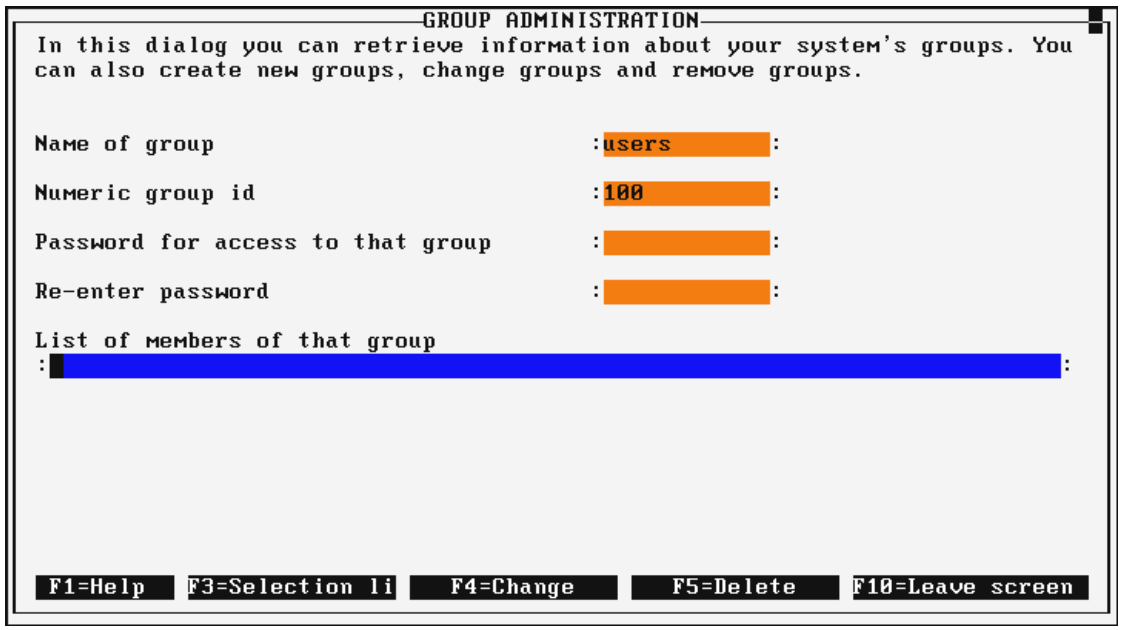


Figure 97. YaST: group administration window

Each user group has a unique name and ID. The default group for normal users is users. To create a new group, enter the name of the group and press Tab to advance to the next entry field. If you entered a new group name, YaST will automatically assign the next available group ID to this group. You can accept it or modify it to your needs. If this group is not intended to be a primary (default) user group, you can protect it with a password as well. All users that should be members of this group can be entered in the line **List of members of that group** (comma-separated). You can press F3 here to select them from the user list, or you can add them manually. Press F4 to create this group, F10 or Esc to leave this window.

If you want to delete a user group, select the group name with F3 or enter it manually and press F5 to delete it. Please note that this will not delete the user accounts belonging to this group! It will only remove the group

information from the file /etc/groups. To leave the group administration window, press F10 or Esc.

4.5 Network configuration with YaST

A Linux system will in most cases be connected to one or more networks. YaST also offers configuration options to set up your network connection. If you need to connect your host to an Ethernet or token-ring network, you can use YaST to enter the correct networking parameters. If you did not define your network card during the initial installation, or if you added a new network card to your system, you first have to define the correct driver for this device. From the YaST main menu select **System administration -> Integrate hardware into system -> Configure networking device**. From the command line, type the following command to open the network device selection window shown in Figure 99 directly.

```
yast --mask netcard --autoexit
```

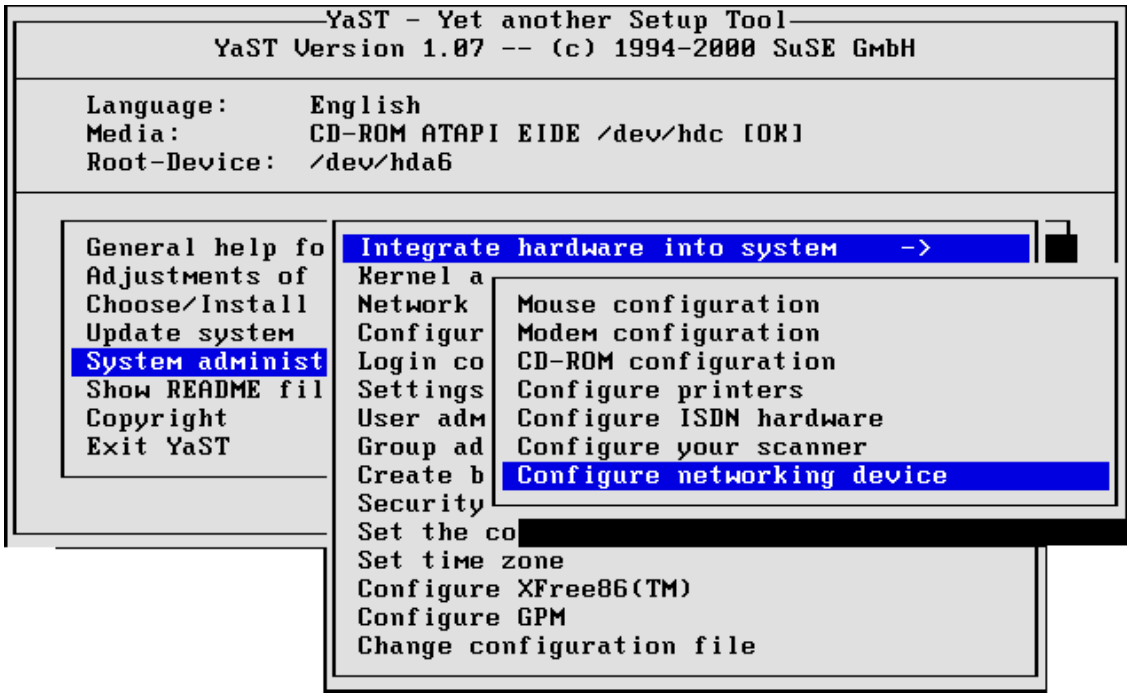


Figure 98. YaST: integrate hardware into system

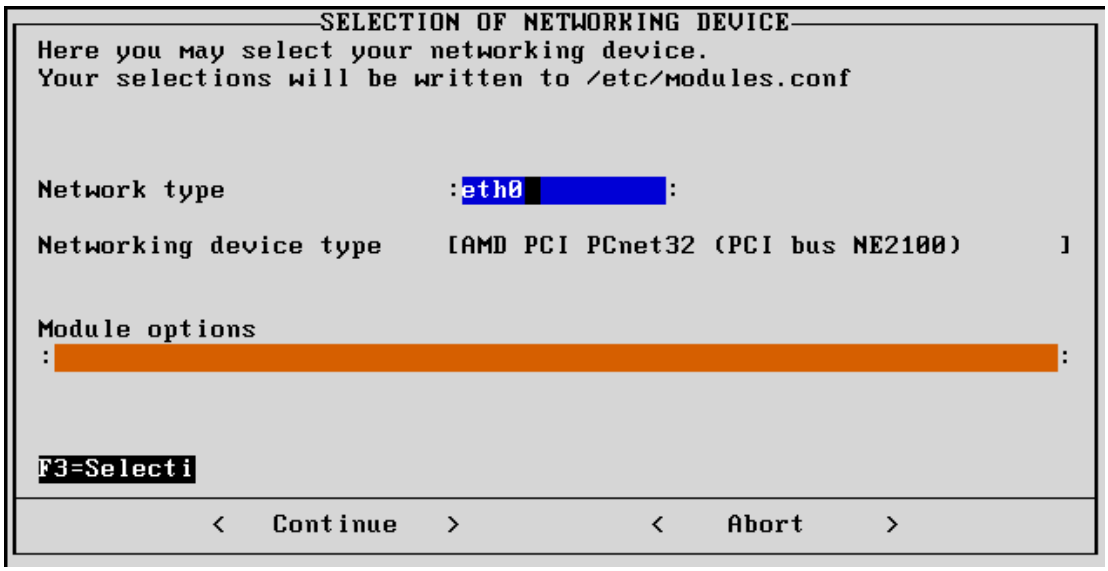


Figure 99. YaST: network device selection

First enter the network type. The two most common ones are Ethernet (for example eth0, eth1, etc.) and token-ring (for example tr0, tr1, etc.). After entering the network type, select the correct driver for this card. Some drivers need additional options; please see Chapter 14, “Kernel parameters” in the SuSE manual for a detailed explanation of the possible values. Most modern PCI network cards do not need any additional parameters, so you can most likely skip this input field. Click **Continue** to finish this configuration dialog. YaST will now add this line to the kernel module configuration file /etc/modules.conf.

After you defined your network type, return to the YaST System administration menu.

Now you can define the networking parameters for this device. Select **System Administration** -> **Network configuration -> Network base configuration**. Alternatively, type the following command at the shell prompt to jump directly to the window shown in Figure 101:

```
yast --mask network --autoexit
```

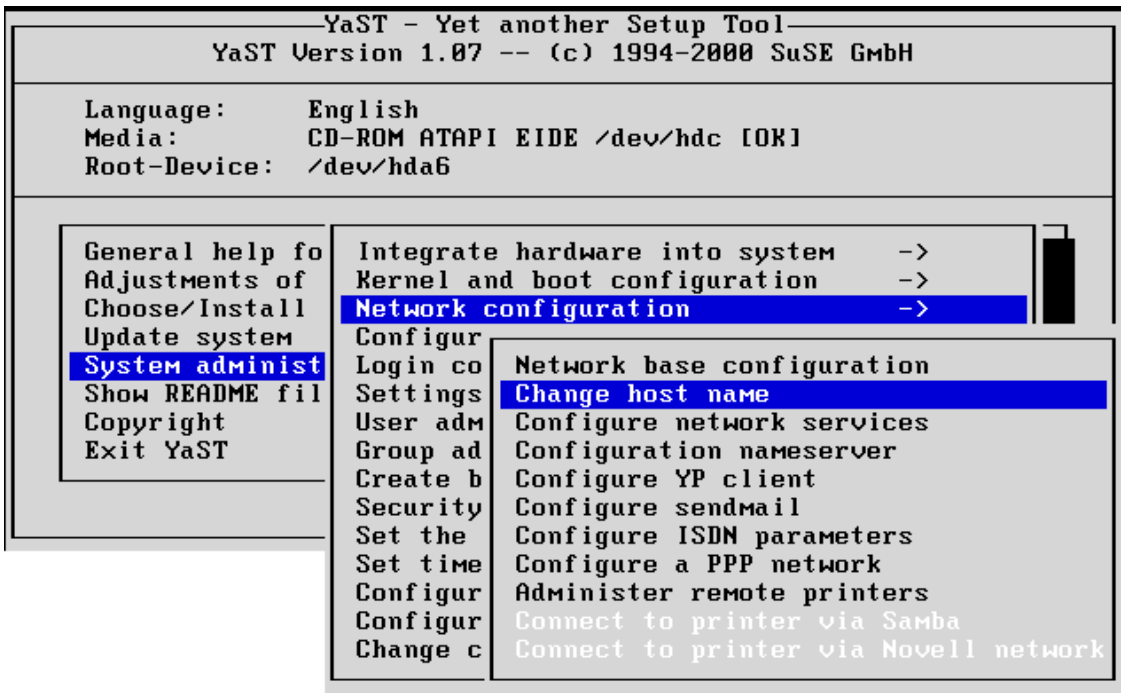


Figure 100. YaST: network configuration options

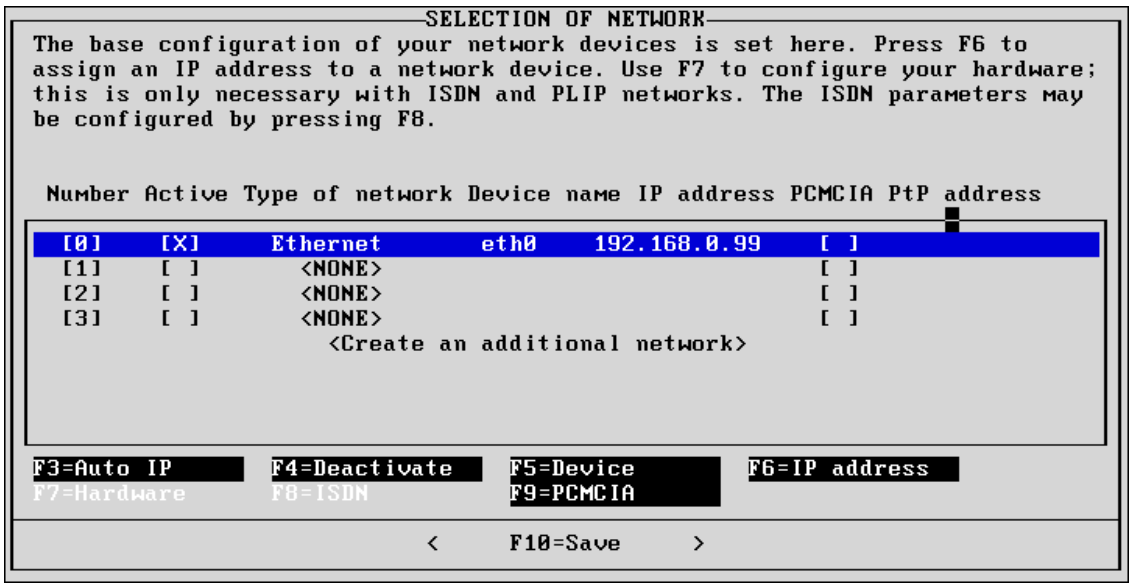


Figure 101. YaST: network base configuration

This configuration window allows you to assign IP addresses to network devices. If you have not configured your network device before, select the type of network first.

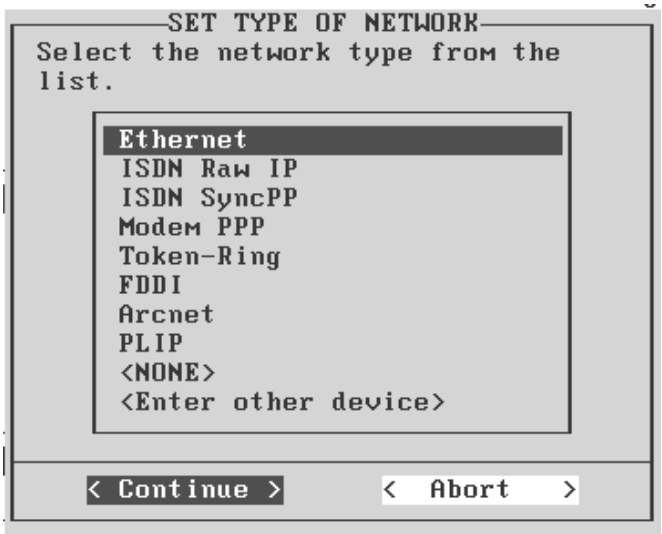


Figure 102. YaST: Set Type of Network window

Figure 102 shows the Set Type of Network selection box. Select the corresponding type for your network card and confirm the selection with **Continue**.

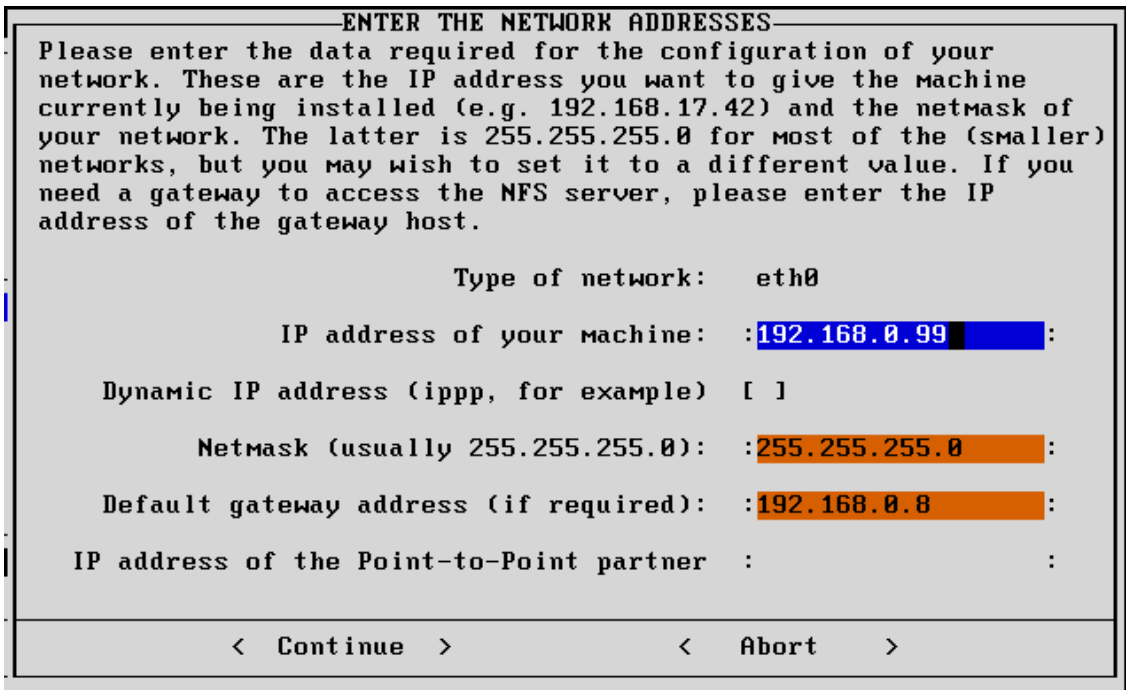


Figure 103. YaST: IP address configuration

After you have defined the network type, you can assign an IP address to this device. Press F5 to open up the dialog shown in Figure 103. Enter the IP address, Netmask and default gateway address, if necessary. Close the dialog box with **Continue**. If you configured a PLIP or ISDN device, you may also have to configure some additional hardware parameters by pressing F7.

If you have more than one network card, you can add it to the free lines below. If you need to add more than the predefined four lines, highlight **Create an additional network** and press Enter.

You can also use this dialog, if you want to assign more than one IP address to a single network card (IP aliasing). To do this, press F5 to select the type of network and choose **Enter other device**.

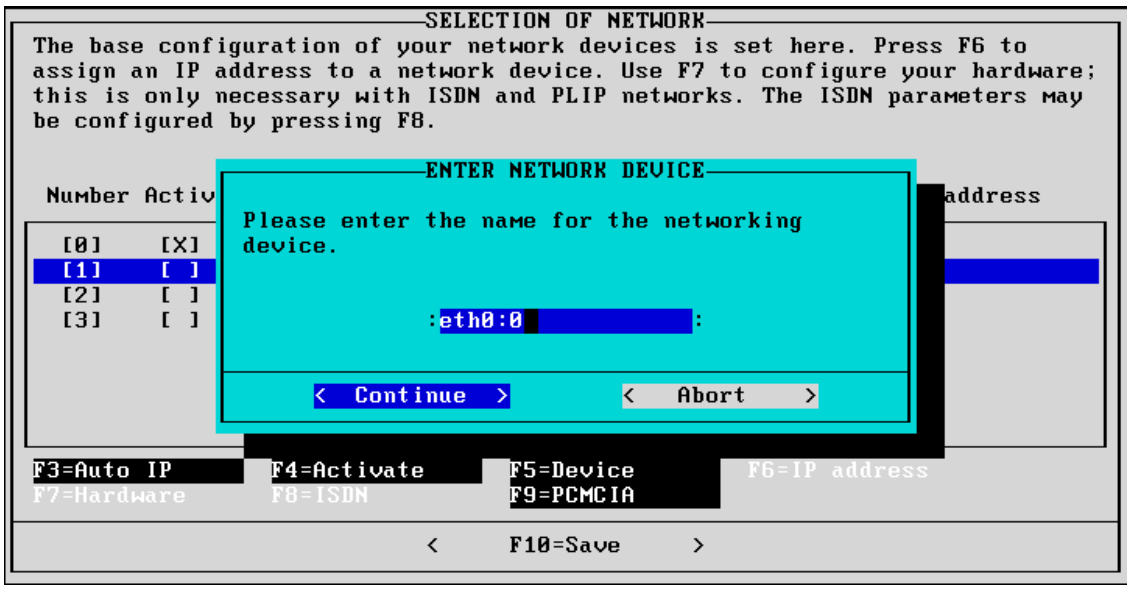


Figure 104. YaST: enter another network device

You can add multiple IP addresses to one Ethernet card, by configuring it as eth0:0, eth0:1 and so on (IP aliasing support must be activated in the Linux kernel; the default SuSE kernel has been compiled with IP aliasing support).

After you have finished the network configuration, press F10 to save the current setup. YaST will now create the respective entries in /etc/rc.config and the network setup will be applied after the next reboot or after restarting the network and routing scripts.

4.6 Changing the configuration file with YaST

SuSE Linux utilizes a central configuration file /etc/rc.config to store most of the system configuration information. The contents of this file will be used by the init scripts on bootup, as well as for creating configuration files for the different services.

The format of this file is plain ASCII text. The configuration is stored in variables in the form VARIABLE=value. Additional comments are marked with a “#” at the beginning of the line. Since rc.config contains most of the configuration information, you do not need to edit the original configuration files for most services. It is sufficient to make the change in this single file; YaST (in combination with the SuSEconfig script collection) will take care of the correct creation of these files. However, if you are used to modifying the

separate configuration files directly, you may still do so. SuSEconfig will detect the manual change and will not overwrite them. Instead you will receive a notification that SuSEconfig has detected a manual change and will create its version of this file in <filename>.suseconfig. You are free to manually implement the changes from SuSEconfig to your file.

If you want to edit variables in rc.config, you can open it in a normal text editor. Each variable has some lines of comments above its definition to give you an overview of the meaning of it. These variables are also covered in section 17.6 “The variables in /etc/rc.config” in the SuSE manual. After you have modified entries in rc.config, you have to run the script SuSEconfig afterwards to apply the changes to the different configuration files.

Alternatively, you can use YaST as a handy front end to edit these variables. From the YaST main menu, select **System administration -> Change configuration file**. To go directly to this dialog from the command line, invoke YaST with the following parameters:

```
yast --mask rcconfig --autoexit
```

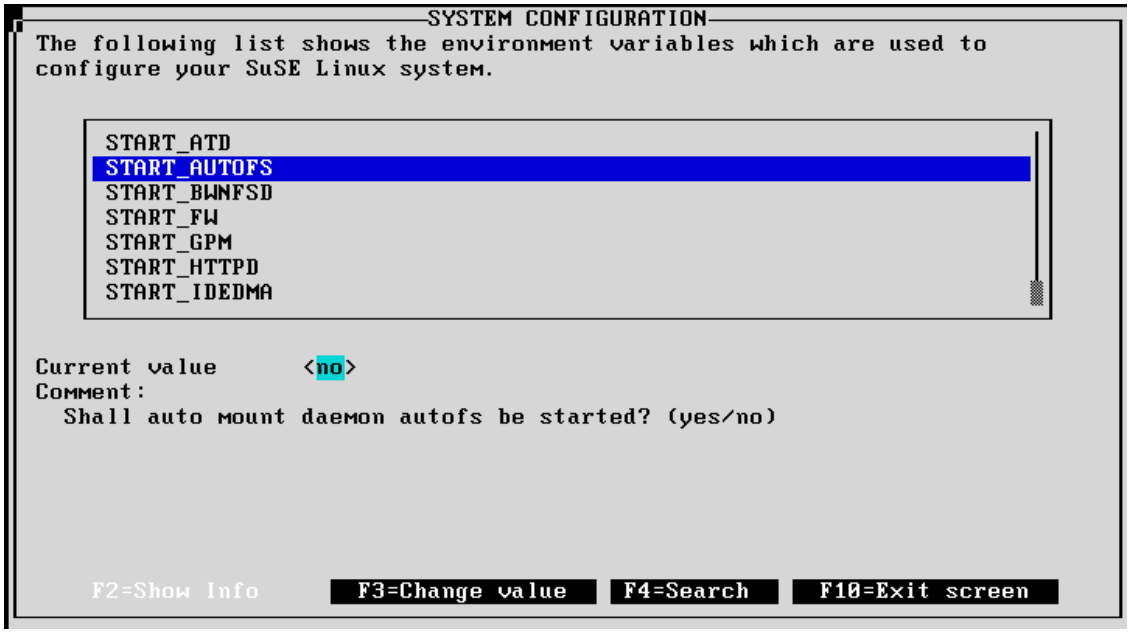


Figure 105. YaST: view the system configuration file

Use the cursor keys to highlight the desired variable. F2 gives you a description of the currently highlighted option.

To search for a certain keyword (case-sensitive), press F4 and enter the desired search term.

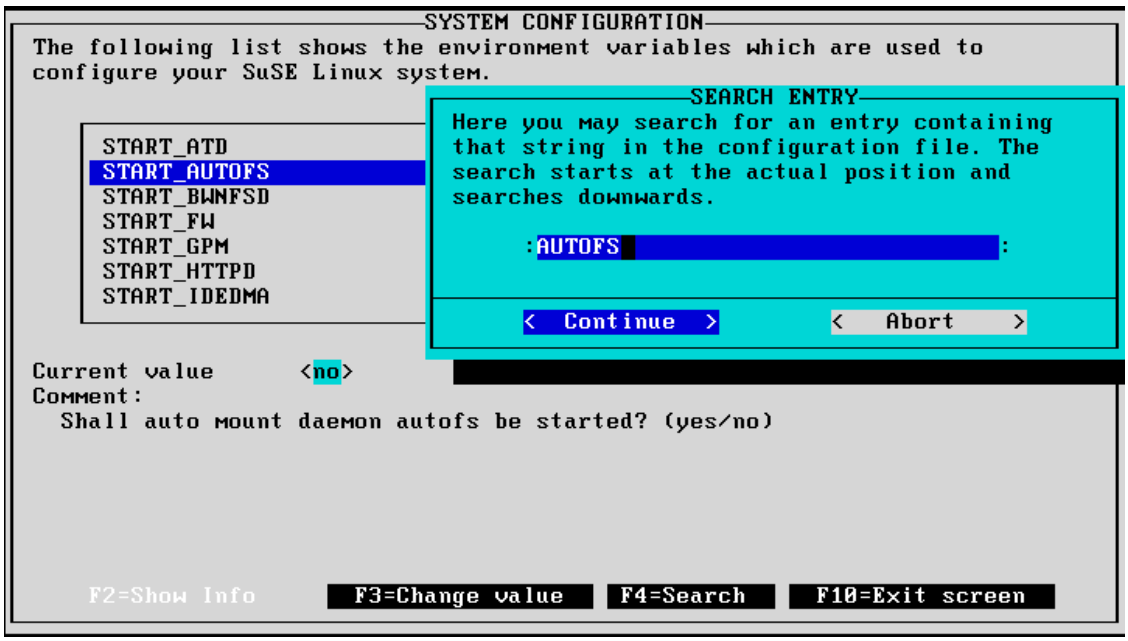


Figure 106. YaST: search for keyword in configuration file

To modify the selected entry, press F3 and enter the new value in the dialog box.

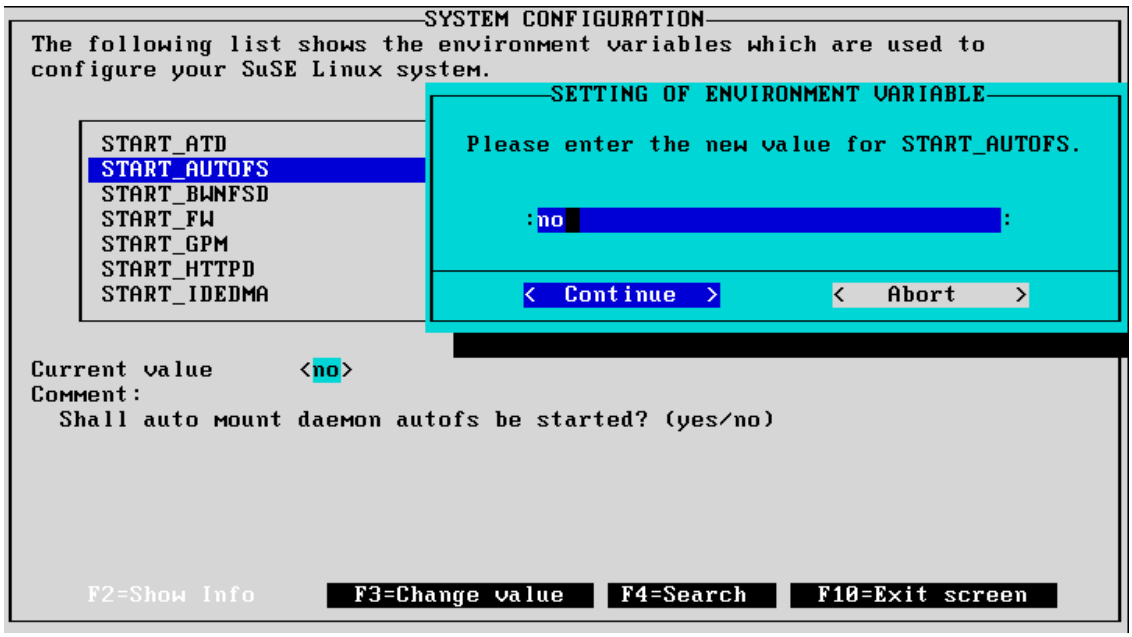


Figure 107. YaST: editing a variable in rc.config

Press F10 to finish the editing and return to the main menu after saving the changes in /etc/rc.config.

4.7 System administration with Yast2

If you prefer to use a GUI to administer your system, Yast2 is the answer. It has an easy-to-use point-and-click interface to allow first time UNIX administrators to configure a server quickly and efficiently.

Yast2 is a shell that holds a collection of modules (not to be confused with kernel modules). These modules provide the GUI component to configure a certain part of your Linux system.

Yast2 is a relatively new SuSE application, and more modules are added with every SuSE release. If Yast2 is not capable of configuring a part of the system that you wish to maintain, either use Yast1 or configure the service manually.

The SuSE technical manual details a wide range of administration procedures, and as such should be consulted if you are unsure of a procedure.

4.7.1 Yast2: Main window

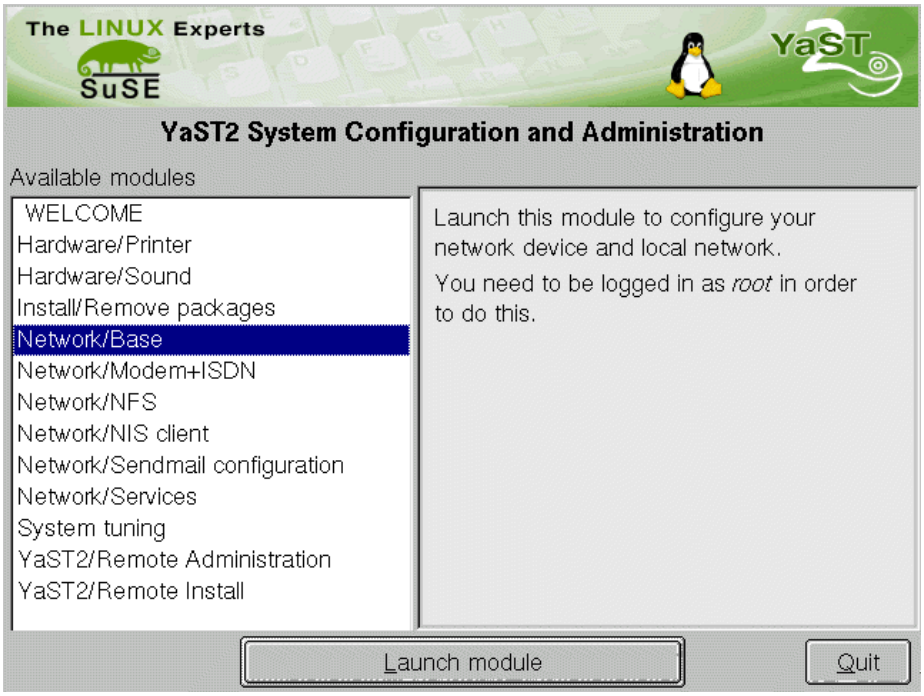


Figure 108. Yast2: Main window

Yast2 is an X-Windows application, so before you begin you need to have loaded up X before we can proceed. To load X-Windows, at the command prompt type:

```
startx
```

Note

To set up your system to boot into X-Windows instead of the console, see Section 3.6.5 Login Configuration in the SuSE manual.

Once you have loaded X-Windows, click the **Yast Menu** button on the bottom of the window (it is a gecko with a hammer and spanner behind it). Select **Yast2 - All Yast2 modules**. You will be presented with the window in Figure 108.

The left-hand pane of Yast2 shows what you can configure on your system:

- **Hardware/Printer** - Configure your printer. This can be a Novell, parallel port, USB, network, or SAMBA (Windows) printer.
- **Hardware/Sound** - Configure your sound device.
- **Install/Remove Packages** - Add and remove packages from your system.
- **Network/Base** - Configure your network settings, including network devices and IP addresses.
- **Network/Modem+ISDN** - Configure your modem or ISDN adapter, including device configuration and ISP configuration.
- **Network/NFS** - Maintain NFS exports and NFS imports for the system.
- **Network/NIS client** - Configure your machine as a NIS client.
- **Network/Sendmail configuration** - Set the behavior of sendmail on the server.
- **Network/Services** - Create, modify and remove network services from the server. This is commonly known as *inetd.*
- **System Tuning** - Speed up techniques for your system. At the moment this only allows IDE disk performance increase via UDMA settings.
- **Yast2 Remote Administration** - Allows you to administer another SuSE server from a central location.
- **Yast2 Remote Install** - Allows you to install SuSE on another computer via a serial port.

We will discuss the most useful aspects of Yast2 to a user installing on a server configuration.

4.7.2 Yast2: Network configuration

To start a module, select it from the left-hand pane shown in Figure 108 and click **Launch Module**.

Our first Yast2 module is the Network/Base configuration module. After selecting the module as detailed above you will be presented with the window shown in Figure 109.

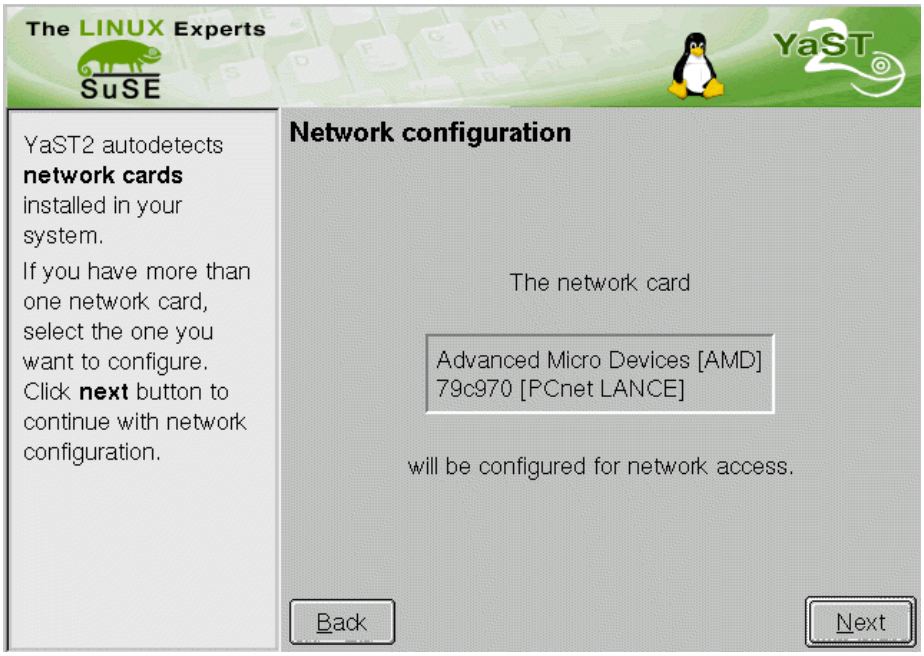


Figure 109. Yast2: Network Base configuration

Yast2 will try to autodetect your network card. If it is unsuccessful, you will have to locate the correct driver for it via the manufacturer. You may also try the SuSE FTP site to see if an update or new driver exists for the card and configure the card manually, depending on the driver.

Once your card has been detected, click **Next** to continue with the network configuration.

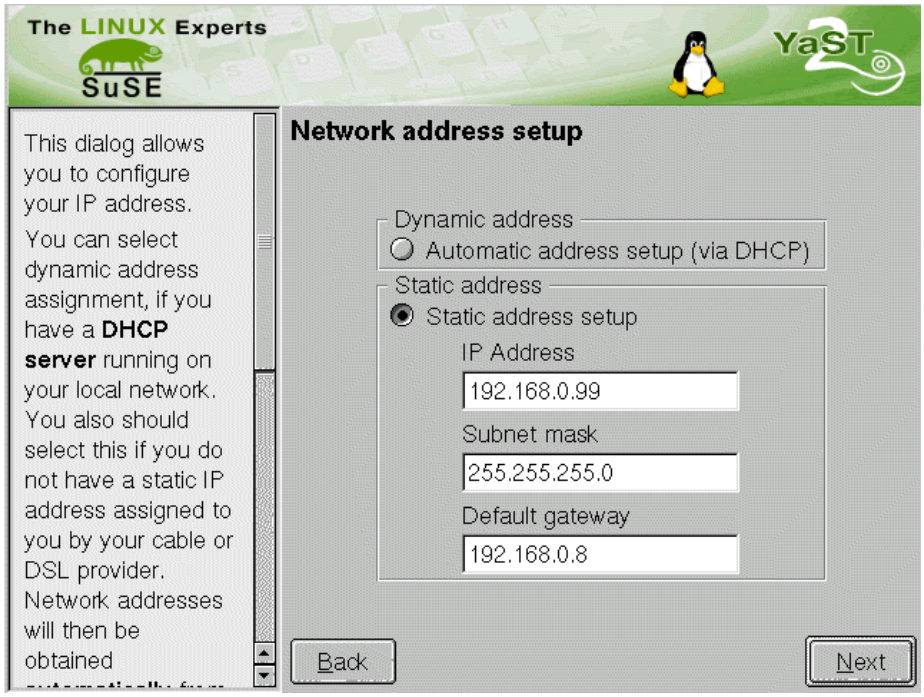


Figure 110. Yast2: Network address configuration

You have two options for configuring your network devices. You can either use DHCP to acquire your network address, gateway address, DNS server and so on, or you can manually assign an IP address to the network interface as we have done in Figure 110.

Once you have entered the corresponding values into the configuration window, click **Next** to continue.

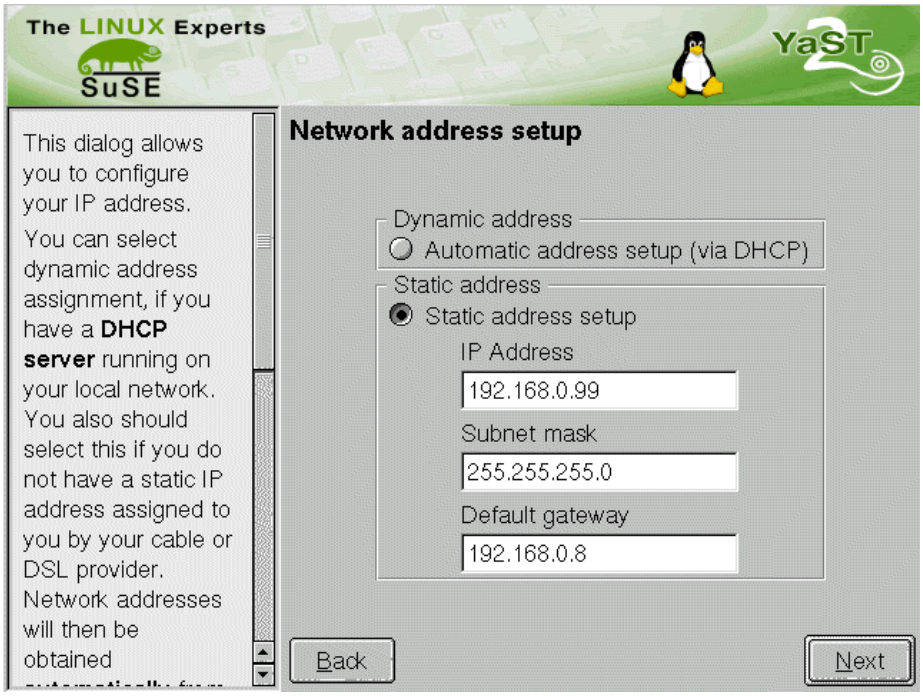


Figure 111. Yast2: Host and DNS configuration

You are now prompted to configure your host name and DNS settings. You can enter up to three domain name servers, referred to *primary, secondary and tertiary* domain name servers respectively. These should point to your DNS server, or your ISPs DNS servers. It is usual to have two domain name servers serve a domain for reasons of redundancy.

The Domain Search List refers to a wildcard list that will be appended to all non-fully qualified domain name (FQDN) names that are sent to the DNS server from this machine. For example, doing a name lookup on *netvista* will be translated to *netvista.ibm.com,* which will be queried against the name server. It allows an easy way to make nicknames for all machines on your network instead of having to type the FQDN.

Click **Finish** to complete the basic network configuration.

4.7.3 Yast2: NFS configuration

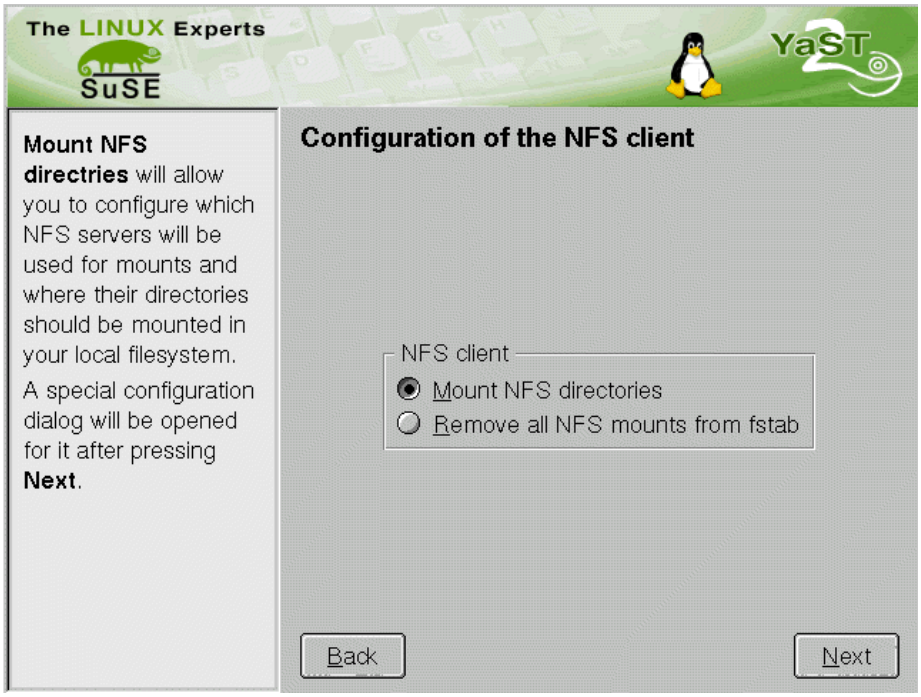


Figure 112. Yast2: NFS configuration

Yast2 allows you to configure the way NFS works on your system.This is either as a server, that allows you to share files among other machines, or as a client, that requests shares from a server. You are given the opportunity to configure both of these using the Yast2 NFS module.

To create a configuration to mount NFS shares, select **Mount NFS directories** and click **Next**. To remove all NFS mounts from your system, select **Remove all NFS mount from fstab**.

If you selected **Mount NFS directories** you will see Figure 113; otherwise you will see Figure 114.

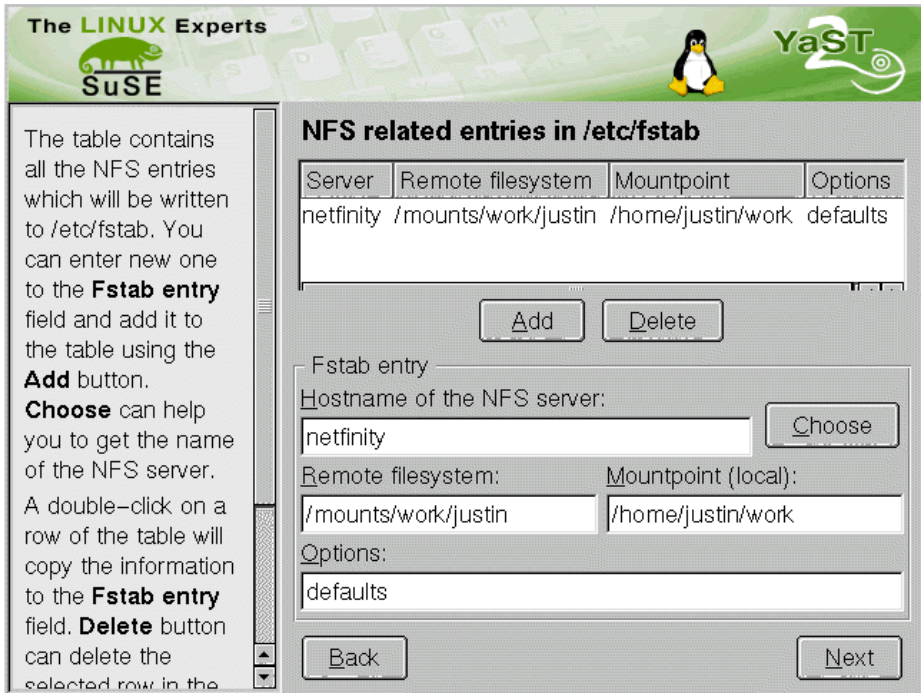


Figure 113. Yast2: Adding an NFS mount

Figure 113 is the window that allows you to configure NFS shares to be mounted by your system.

You must enter all the relevant information in this window and press **Add** to enable the share. Repeat this process until all of the NFS shares you wish to use are entered.

The entries are as follows:

- **Hostname of the NFS server** - This is the IP address or host name of the NFS server that you wish to mount the directories from.
- **Remote filesystem** - This is the remote directory on the server that you wish to request to share. It must be a fully qualified directory name, starting from the root (/) directory.
- **Mountpoint (local)** - This is the local directory that you wish to mount the remote directory under.
- **Options** - This allows you to set certain options for the mount point. Please look at the mount (8) man page for details of the options you can use.

Once you have entered all the mount points you wish to use, press the **Next** button to continue.

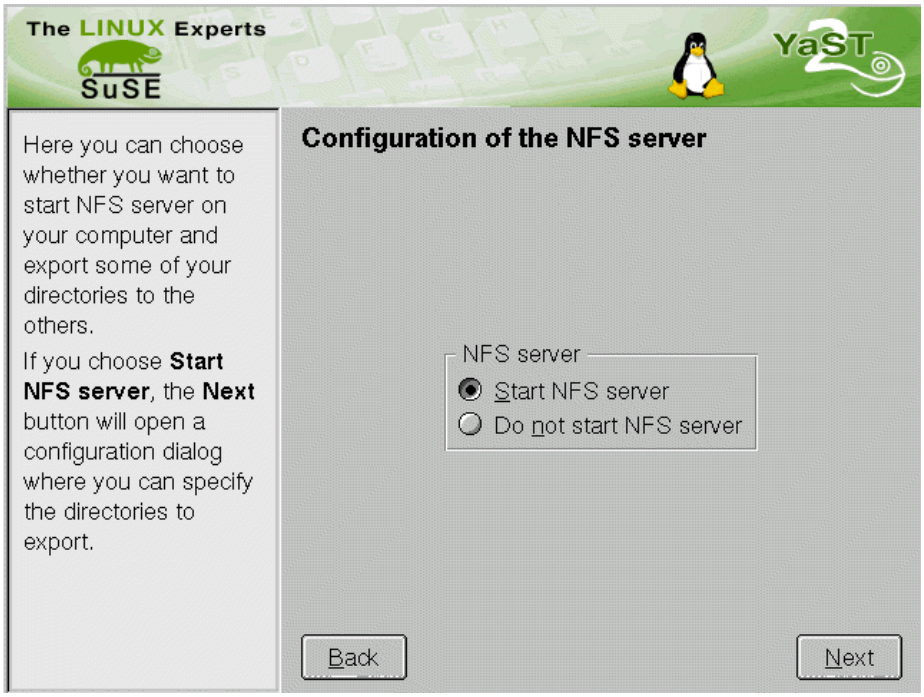


Figure 114. Yast2: Starting the NFS server

You now have the opportunity to start the NFS server to allow you to share your directories with other computers on the network. If you do not wish to share any directories with other machines, select **Do not start NFS Server** and press **Next** to continue. If you do want to share NFS mounts with other computers, select **Start NFS server**, and press **Next** to continue.

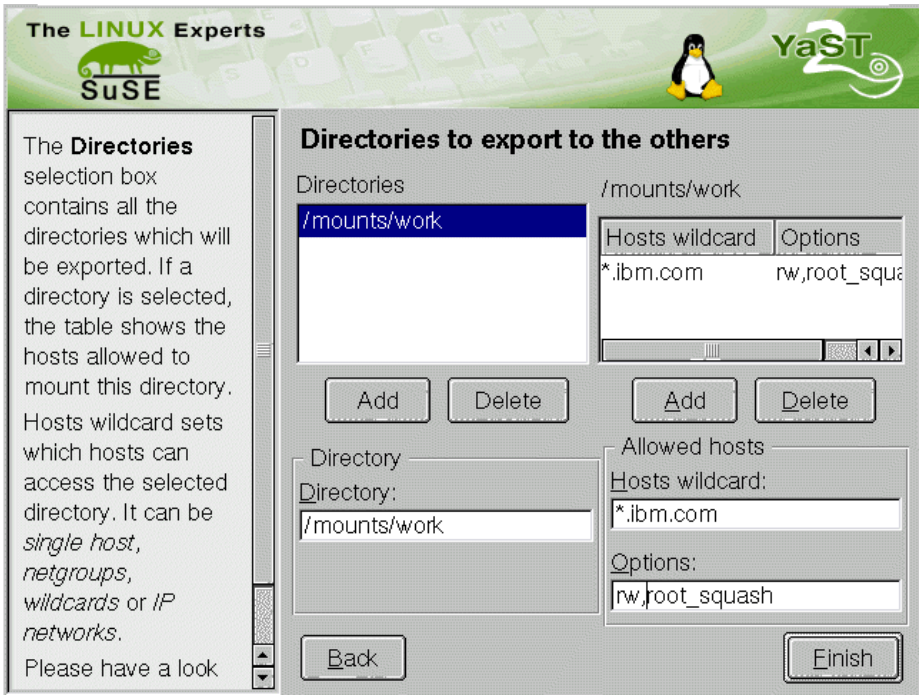


Figure 115. Yast2: Adding NFS mounts

To export your directories to other machines you have to tell the server about the directory you wish to share, who is allowed to access the directory, and under what restrictions. Figure 115 shows you how to enter this data.

As with the previous example, you must enter all the relevant data for the share, and press **Add** before proceeding with the configuration. The only difference is that you have two Add buttons.

When exporting NFS share, you are allowed to explicitly specify which hosts are allowed to access the shared directories. Yast2 allows you to keep on adding hosts that are allowed to access the specified share (in the left-hand pane). You first of all have to configure the share before imposing restrictions on who can use it. There is only one option for this, and that is **Directory**. The directory statement simply tells the NFS server what directory you wish to share. Make sure the directory exists; otherwise the server will behave erratically.

Once you have allocated a directory to share, you can start allocating its share restrictions.

The NFS server will allow host name wild cards to say a certain network can access the shares. In our case we have enabled the IBM network to access these shares by specifying **.ibm.com* as the allowed hosts.

The options section tells the server how the restrictions impose the mount on the NFS clients. This only applies per restriction, not to every client that accesses the NFS shares. For example, if we added *.suse.de to the restrictions table, we could allow everyone at IBM to have write access to the share (option **rw**), but read-only access to everyone at SuSE (option: **ro**) for the same share.

See man export(5) for other options you can use.

Once you have added all of the mounts you wish to export, click **Next** to continue. You will be asked to confirm that you wish to use these settings. If you wish to edit them some more, click **No;** otherwise click **Yes** to commit them.

4.7.4 Yast2: Network services configuration

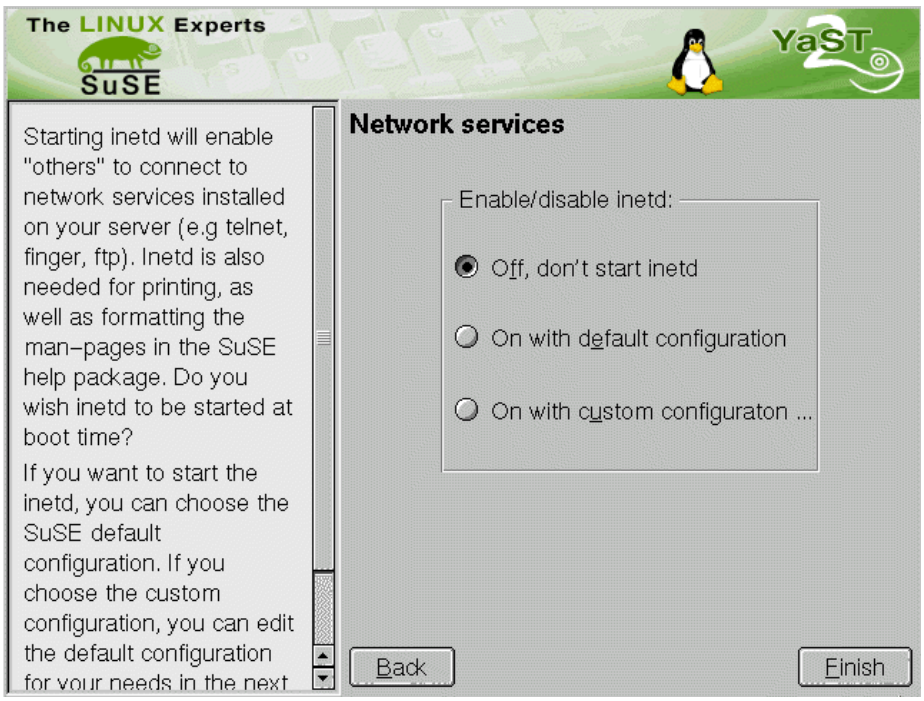


Figure 116. Yast2: Configuration of inetd

You can stop inetd from running at system bootup, by selecting **Off, don't start inetd**. You can use the default configuration, by selecting **On with default configuration**. Or, you can configure inetd yourself by selecting **On, with custom configuration...**

We will guide you through editing the inetd configuration to allow you to add or remove services from your server.

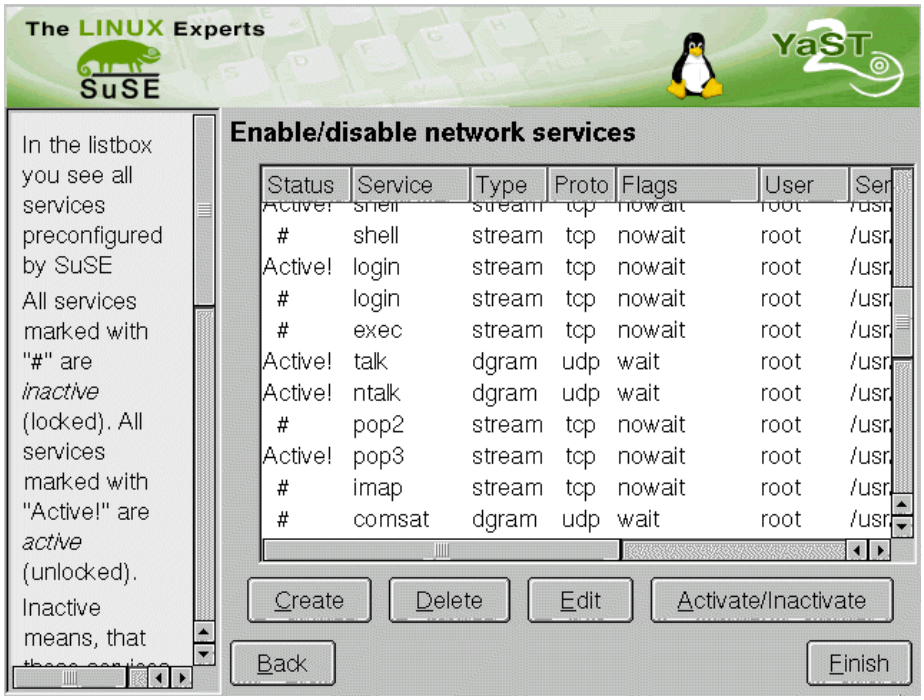


Figure 117. Yast2: Editing the inetd configuration

You have four options while editing the inetd configuration:

- **Create** - This allows you to add a new service to the server.
- **Delete** - This will delete the selected service from the system.
- **Edit** - This allows you to edit the currently selected service.
- **Activate/Deactivate** - This will stop the service, but will not delete the entry. This has the same effect as deleting the entry, but will not remove it from the configuration file. If it activates the service, it will take it out of the deactivated state and allow it to run.

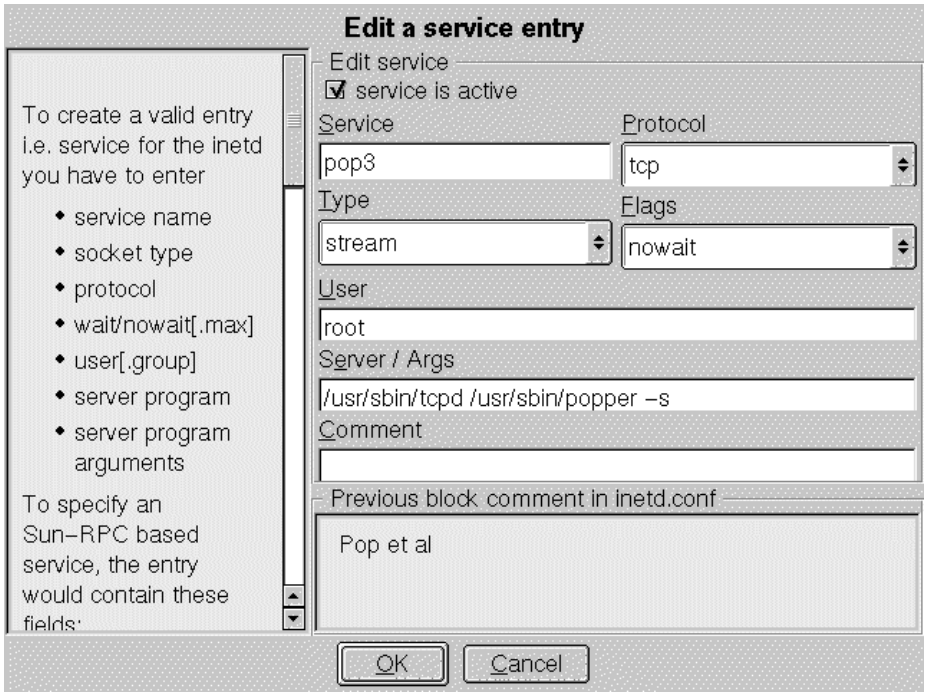


Figure 118. Yast2: Add/configure a service

Figure 118 will be loaded if you click the **Add** or **Edit** button in Figure 117. It allows you to add a service entry, or edit an existing one. The options are exactly the same for both configuration type:

- **Service** - This is a service name that is defined in /etc/services. This file holds information, such as port number, service type, service name and so on, regarding a certain service. You should enter an existing service name (as defined in /etc/services) here.
- **Protocol** - This defines what protocol this service uses. The most popular protocol types are TCP, UDP, and ICMP. The protocol defined must be present in /etc/protocols.
- **Type** - This defines the type of the connection that will be used. This can be one of **stream** (stream type)**, dgram** (datagram type), **raw** (raw socket type), **rdm** (reliably delivered message type) or **seqpacket** (sequenced packet type).
- **Flags** - There are two options for this item. **Nowait** is usually selected for servers that use the type `stream`. It allows the service to accept new requests while processing other requests. The service is known to be “multi-threaded”. **Wait** is used to allow only one connection at a time to the

service. It is known to be “single-threaded”. Check the documentation of the service to see how it should be configured.

- **User** - This specifies under what user the service should be run. It is usually root, but it is imperative that you check the documentation of the service you are configuring, since running services under the wrong user (that user being root) can cause major security issues.
- **Server/Args** - This is the command to run the service, along with the arguments it takes. Consult the documentation of the service to find out what arguments it takes, and what those arguments do.
- **Comment** - This allows you to set a comment for this service. It is always a good idea to comment services so that you can remind yourself and others about what the service does, or special warning for other administrators.

4.7.5 Yast2: Package maintenance

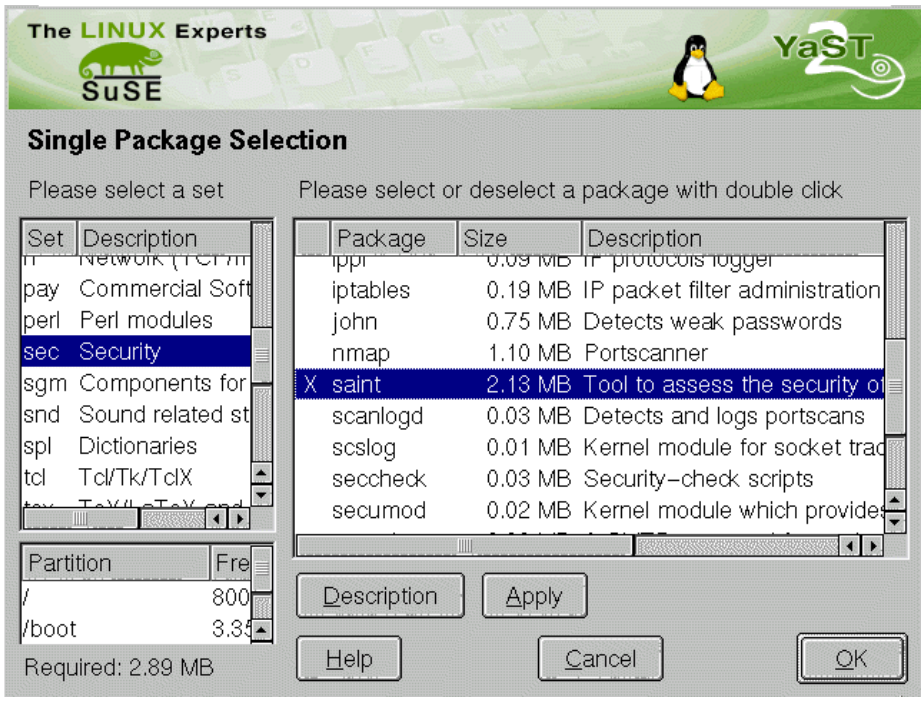


Figure 119. Yast2: Package installation

Selecting **Install/Remove packages** will allow you to install and remove packages from the system.

The left-hand pane allows you to select the package series from the installation medium. To install a package, just double-click the package name, or click **Apply** and an X will appear next to it. To remove an installed package, again double-click it: this time a d will appear next to it. This signifies that the package is marked for deletion.

To read the package description, select the package and click **Description**. This will bring up a window that will give you a short description of what the package does.

There are some combination of packages that are inadvisable to install together. If this situation arises, you will be told about the problem. The same is true if a certain package depends on other packages to run.

4.8 Finding Linux commands

You may want to run a Linux program from the command line prompt. If so, there are several directories that contain commands that you can run. You can run these without needing to know where they are because your search path includes a number of directories that will be searched whenever you try to execute a command. The search path is given by the environment variable $PATH. You can view the content of this variable by running the following command:

```
echo $PATH
```

If you want to find out where a command is located, execute the command:

```
whereis command_name
```

where `command_name` is the command you are looking for. If you want to find the command `yast` you can execute:

```
whereis yast
```

This will give you the following results:

```
yast: /sbin/yast
```

You notice that this command is located in the /sbin directory. Many of the major administrative commands will be found in the /sbin and /usr/sbin directories.

Another helpful command for finding files on your system is `locate`. The `locate` command will also list files that match the search name, if they are not in your current search path. To search for all README documents on SuSE Linux run the following command:

```
locate README
```

Since this will be a huge amount of output, you might want to redirect the ouput to a text pager such as `less` or `more`:

```
locate README | less
```

This will enable you to look at the output page by page. Press q to leave `less` and return to the command line.

Note

SuSE Linux automatically runs `updatedb` once every 24 hours. If you cannot find what you are looking for, run `updatedb` from a command line.

4.8.1 File system permissions

Linux has inherent security features, the most noticeable being file system permissions. Setting permissions on files allows the system administrator to restrict access to parts of the file system.

File permissions can be set on files and directories. The easiest way to see an example of this is looking in the /home directory:

```
mail:/home # ls -l
total 1
drwxr-xr-x  19 root     root          396 Nov 15 21:06 .
drwxr-xr-x  22 root     root          467 Nov 13 16:28 ..
drwx------   6 davej    users         912 Nov 15 21:05 davej
drwx------   6 george   users         912 Nov 15 21:03 george
drwx------   6 ivo      users         912 Nov 15 21:02 ivo
drwx------   6 jakob    users         912 Nov 15 21:03 jakob
drwx------   6 jasmin   users         912 Nov 15 21:04 jasmin
drwx------   6 jens     users         912 Nov 15 21:04 jens
drwx------   6 jhaskins users         912 Nov 15 21:02 jhaskins
drwx------   6 justin   users         912 Nov 15 21:06 justin
drwx------   6 lenz     users         912 Nov 15 21:03 lenz
drwx------   6 linux    users         912 Nov 15 21:03 linux
drwx------   6 malcom   users         912 Nov 15 21:04 malcom
drwx------   6 rachael  users         912 Nov 15 21:03 rachael
drwx------   6 rafiu    users         912 Nov 15 21:04 rafiu
drwx------   6 ruediger users         912 Nov 15 21:04 ruediger
drwx------   6 rufus    users         912 Nov 15 21:02 rufus
drwx------   6 ted      users         912 Nov 15 21:03 ted
drwx------   6 uzi      users         912 Nov 15 21:04 uzi
mail:/home #
```

Figure 120. Viewing file permissions

Taking the user **linux** as an example:

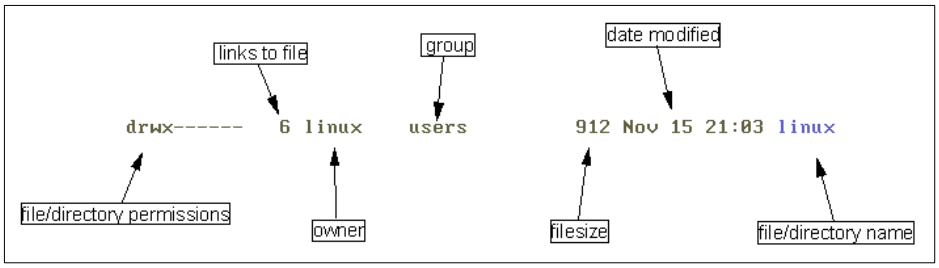


Figure 121. Explanation of ls output

What we are most interested in is the file/directory permissions. This signifies a lot of information in a short amount of space:

d - The first character in the permissions signifies that this is a directory. Other files are represented by:

- - a normal file.

l - a symbolic link to another file.

c - refers to files in the /dev directory. This signifies the file represents a character device.

b - refers to files in the /dev directory. This signifies the file represents a block device.

rwx - In this case it allows only the owner of the file (in this case linux) to read, write and execute this file.

Type	Owner	Group	World
d	rwx	---	---

As you can see, the format of the string is becoming a bit easier to understand.

The owner of the file is the user that created the file. The group part is the group that owns the file (for example, the group *users*). The world part means everyone else. Setting a permission in the world part sets the permission for every user, irrelevant of their group membership and so on.

Here is another example:

```
-rwxr-xr--
```

This means that this is a normal file, the owner can read, write and execute the file, the group can read and execute the file, and everyone else can read the file, but not modify or execute it.

As for directories, if you set a directory as:

```
drwxrw-rw-
```

you are saying that only the directory owner is allowed to execute something "inside" the directory. So if another user tries to change directory (cd) into this directory, they will get a "permission denied" error message. This is exactly what happens with regards to user's home directories.

To change the permissions on a file, you use the `chmod` command. Only *root* users can modify files that do not belong to them. You must own the file to be able to change its permissions.

The easiest way to change permissions is to use symbolic representations of what you want permissions to be.

Note

The other way to represent file permissions is to use octals. For more information about this and the `chmod` command see the chmod man page.

```
chmod g+rw myfile
```

This is one of the simplest ways of changing a permission. You are saying that you want the file `myfile` to allow all members of the group to be able to read and write to it.

If you used a **-** (minus sign) instead of a plus, you would be taking away those permissions. This would mean that members of the group would not be allowed to read or write to the file.

You can mix adding and removing permissions in the same command:

```
chmod u+x-rw myfile
```

This will allow executing the file, but will not allow reading or writing the file for the file owner.

Here is a summary of the symbolic representations available in `chmod`:

r - read

w - write

x - execute

- - take away the permissions

+ - add the permissions

s - set the SUID bit. This says that if the file is executable, it will be run as the owner of the file, not as the user that is running the file.

Chapter 5. TurboLinux basic system administration

Linux follows the conventional UNIX model of storing configuration information in plain text files under the directory /etc. Many of these files are human readable, and many others can be understood with a little experience with the system. However, it is quite time consuming and confusing to try administering a Linux server by directly editing files in /etc, at least until you are more experienced. For this reason, we will emphasize the tools TurboLinux provides to make administration more convenient and understandable to novice and intermediate Linux users, while at the same time pointing to the actual files in /etc being modified.

5.1 Configuring X with most Netfinity and xSeries servers

Current Netfinity and xSeries servers have several versions of S3 video cards that are not fully supported by the version of XFree86 (the X server) that ships with TurboLinux. Therefore, you may encounter an issue of configuring X to work properly. In this section we will start with instructions to configure an X server with the generic SVGA server. We will then give instructions for using the VESA frame buffer server (see 5.1.2, “Installing the VESA frame buffer server” on page 127), a generic driver that will give basic support to any video card.

5.1.1 X-Windows configuration and startup

X-Windows configuration is a process that is still a work in progress. In Appendix B, “Working video modes for IBM Netfinity servers” in the IBM redbook, *TurboLinux Integration Guide for IBM @server xSeries and Netfinity*, SG24-5862 are some of the monitor and video adapter settings you need to be concerned about when setting up your X-Windows system. In order to configure your X-Windows you need to run a tool that will probe the system for information and build or modify a file to include the appropriate information. Two tools available to perform the X-Windows configuration that can run from your Linux command prompt are:

- turboxcfg. This is also called Xconfigurator.
- XF86Setup. This program is a standard X-Windows tool and can sometimes provide information that is different from turboxcfg.

In Figure 122 is an example of executing turboxcfg.

© Copyright IBM Corp. 2001

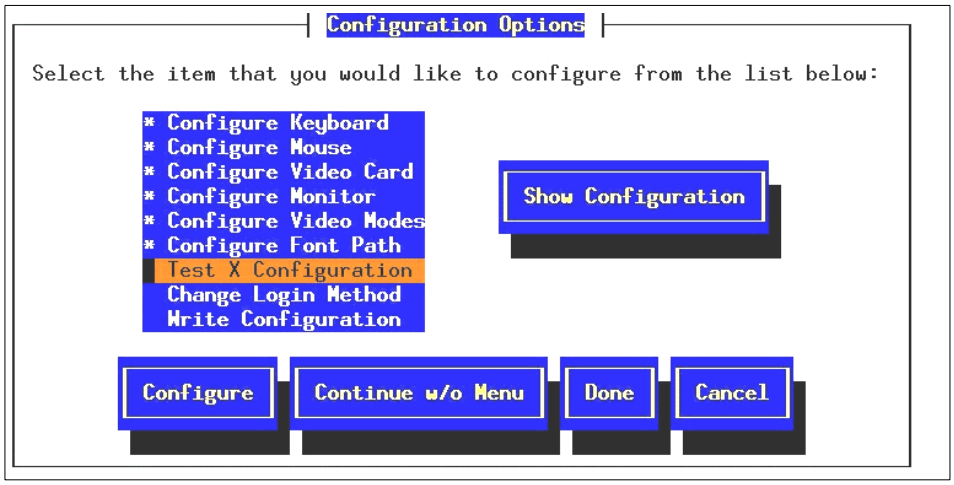


Figure 122. Configuration Options window

It is advisable to start out by selecting **Show Configuration** to see how the system is currently configured.

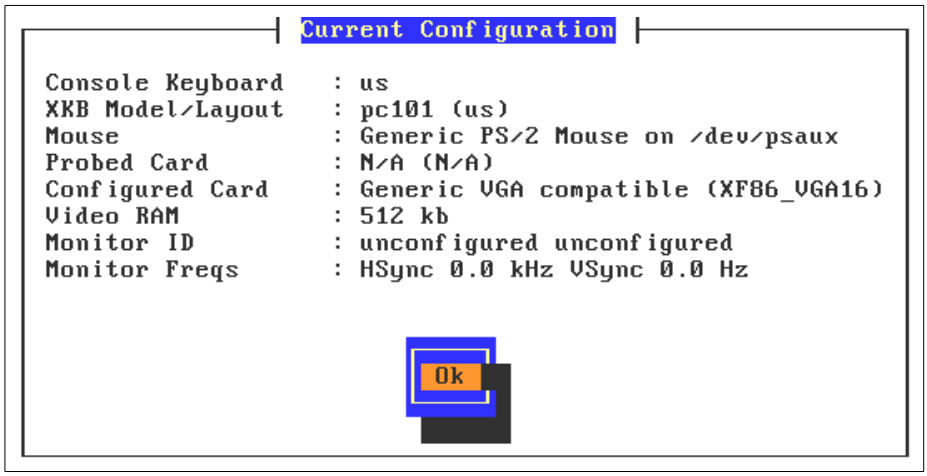


Figure 123. Current Configuration window

Above you see our incomplete configuration left from the install. To properly configure X, follow the following steps:

1. First we must confirm that the correct X server has been installed. Highlight **Configure Video Card** (Figure 123) and press Enter. You will see a window similar to Figure 124.

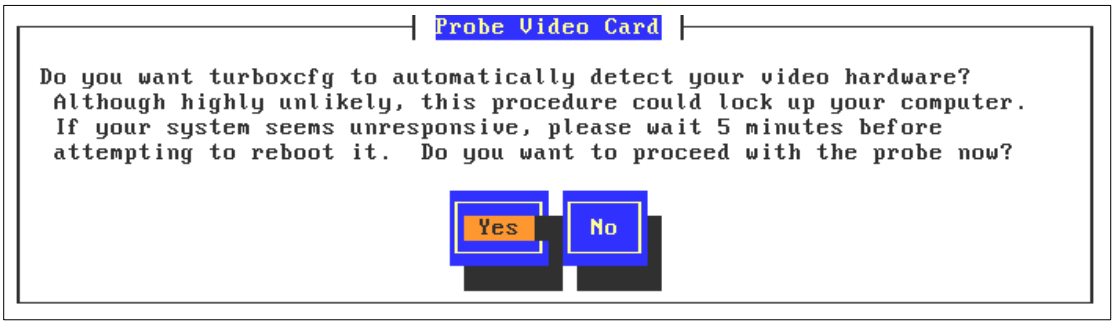


Figure 124. Probe Video Card window

2. Select **Yes** in Figure 124.

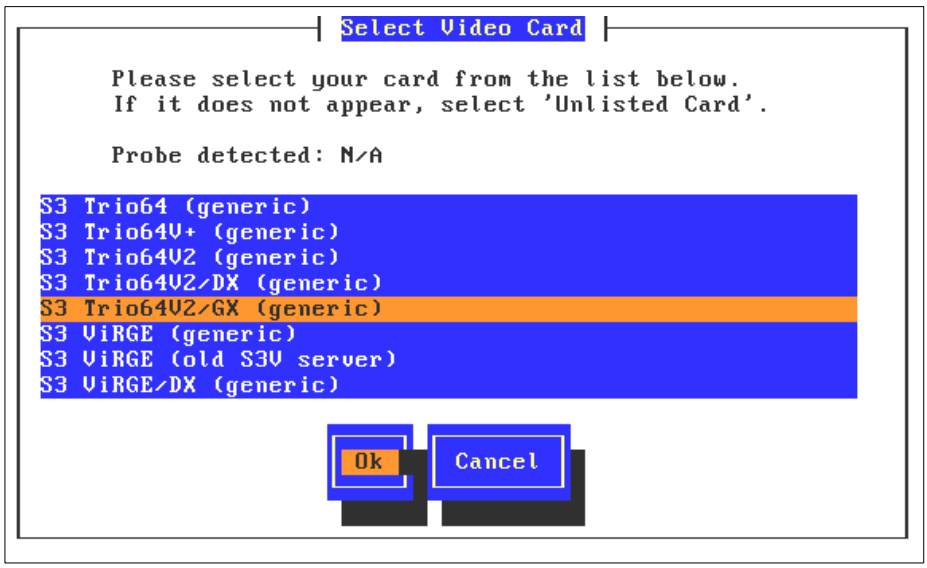


Figure 125. Select Video Card window

3. In Figure 125, note that the card has not been detected but we know that the Netfinity 5000 we are using has a S3 TrioV2/GX video card installed. Therefore, we select it and press **OK**. You will see a window similar to Figure 126.

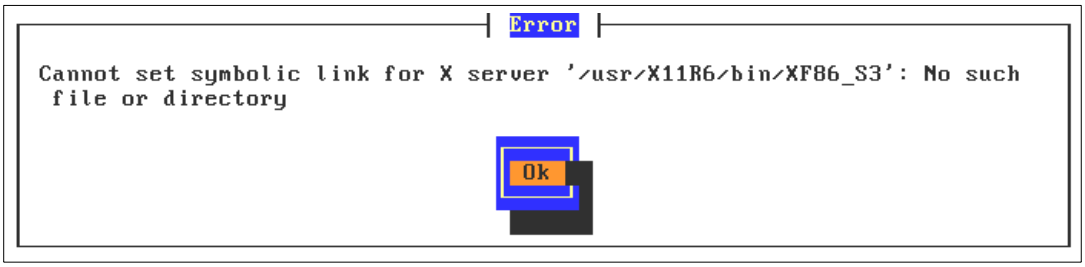


Figure 126. Error window

4. Here the correct X server was not installed, and turboxcfg complains about this fact. The error above indicates that the X server XF86_S3 has not been installed, so we now install it by mounting the TurboLinux 6 CD and installing the file. The commands to do this are:

```
mount /mnt/cdrom
cd /mnt/cdrom/TurboLinux/RPMS
rpm -Uhv XFree86-S3-3.3.6-6.i386.rpm
```

   After the XFree86-S3 package is installed, you will see a window similar to Figure 127.

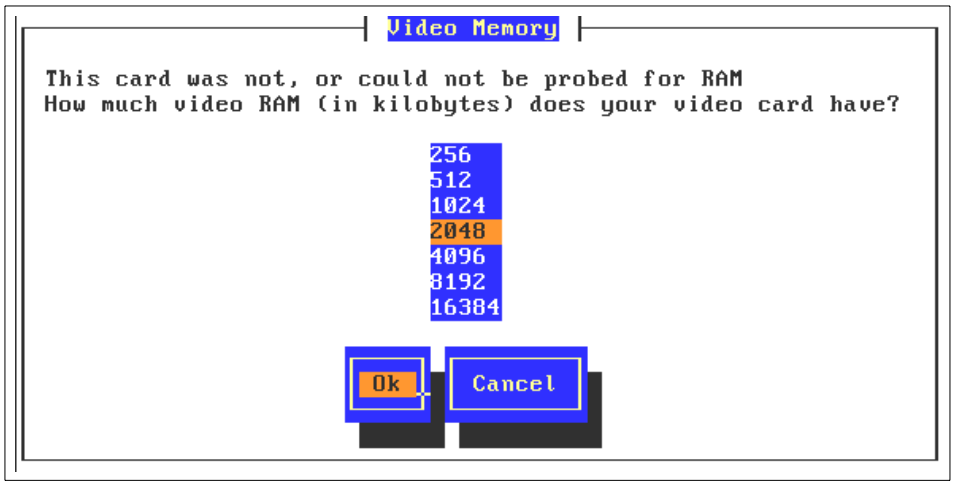


Figure 127. Video Memory window

5. Turboxcfg finds the server and proceeds to ask for the amount of video RAM on the card.

6. Next you should select **Configure Keyboard**. The questions in this section ask which keymap code to use, how many keys are on your keyboard, and the country code to use.
7. Configure Mouse asks for you to specify the type of mouse and number of buttons.
8. Configure Monitor requires you to choose the manufacturer and model of your monitor.
9. Configure Video Modes allows you to set the maximum video resolution and color depth.
10. Configure Font Path allows you to use either 75dpi or 100dpi fonts.
11. Test X Configuration allows you to see if your configuration works properly.
12. If the X configuration works, you can choose **Change Login Method** to change to graphics, or choose to leave it in text mode.
13. After everything has completed successfully, you can select **Write Configuration**, which saves the information to the file /etc/X11/XF86Config.

5.1.2 Installing the VESA frame buffer server

If you have problems configuring the X server, or would like to create an image or process that runs on any video card, you should install the VESA frame buffer driver. The frame buffer is designed to give limited functionality to any VESA compliant video card. The following is a set of instructions needed to configure the frame buffer.

1. With the system started in command mode, log in as "root".
2. Mount the TurboLinux Companion CD and install the frame buffer server package with the following commands:

```
mount /dev/cdrom /mnt/cdrom
cd /mnt/cdrom/TurboContrib/RPMS
rpm -ivh XFree86-FBDev-3.3.6-6.i386.rpm
```

3. Save the current symbolic link and create a new symbolic link by running the following commands:

```
mv /etc/X11/X /etc/X11/X.old
ln -s /usr/X11R6/bin/XF86_FBDev /etc/X11/X
```

4. Open /etc/lilo.conf to add a new entry for the frame buffer server.

```
pico /etc/lilo.conf
```

   The file should look something like this:

```
boot=/dev/sda
map=/boot/map
install=/boot/boot.b
prompt
timeout=50
default=linux
image=/boot/vmlinux
          label=linux
          root/dev/sda1
          initrd=/boot/initrd
          read-only
```

5. Make a copy of the existing entry. Change the label on the new entry to linux-fb or something else intuitive to you. In the new entry, and the line `vga=xxx` (where "xxx" is defined in Table 6) after the image line and change the label so that it is unique.

Table 6. Screen resolution table

Screen Resolution 640x480	Screen Resolution 800x800	Screen Resolution 1024x768	Screen Resolution 1280x1024	Bits/Pixel
769	771	773	775	256
784	787	790	793	32K
785	788	791	794	64K
786	789	792	795	16M

The following example is an entry in /etc/lilo.conf with the frame buffer server installed at a resolution of 800 x 600 and 64K colors:

```
image=/boot/vmlinux
          label=linux-fb
          root/dev/sda1
          vga=788
          initrd=/boot/initrd
          read-only
```

6. Do not change the default image until you have verified that the new image works correctly. Update the master boot record and the LILO boot loader by running the command:

   ```
   lilo
   ```

7. Edit /etc/X11/XF86Config to create a new section screen entry for the frame buffer server. Copy the following example of a screen entry and

make the necessary changes. The corresponding depth value defined by `zzz` is from the table above. `xxxx` and `yyyy` depend on predefined strings in XF86Config. Replace xxxx with the string following the `Identifier` under the `Device` section. Replace `yyyy` with the string following the `Identifier` under the `Monitor` section:

```
Section Screen
Driver fbdev
Device xxxx
Monitor yyyy
Subsection Display
Depth = zzz
Modes default
EndSubsection
EndSection
```

8. Reboot the system and remove all the media.
9. You may receive a virus warning after you restart the server; this warning is normal. Select **Change is expected**.
10. At the LILO boot prompt, press the Tab key for kernel options. You should now have two options: linux and linux-fb. Select **linux-fb**.
11. After the system has restarted in command mode, your can start the X server by issuing command:

    ```
    startx
    ```

12. If this works, you may want to edit /etc/lilo.conf again and make linux-fb the default. However, that is not necessary.

5.2 Turbonetcfg

Turbonetcfg is TurboLinux's multi-purpose network configuration tool. With it you can configure everything from the IP address of your NIC to the Apache Web server. To invoke this tool, type `turbonetcfg`. Although it is a text-mode utility, we recommend that you run it from inside X, since some of the windows require a larger console than is normally available without X.

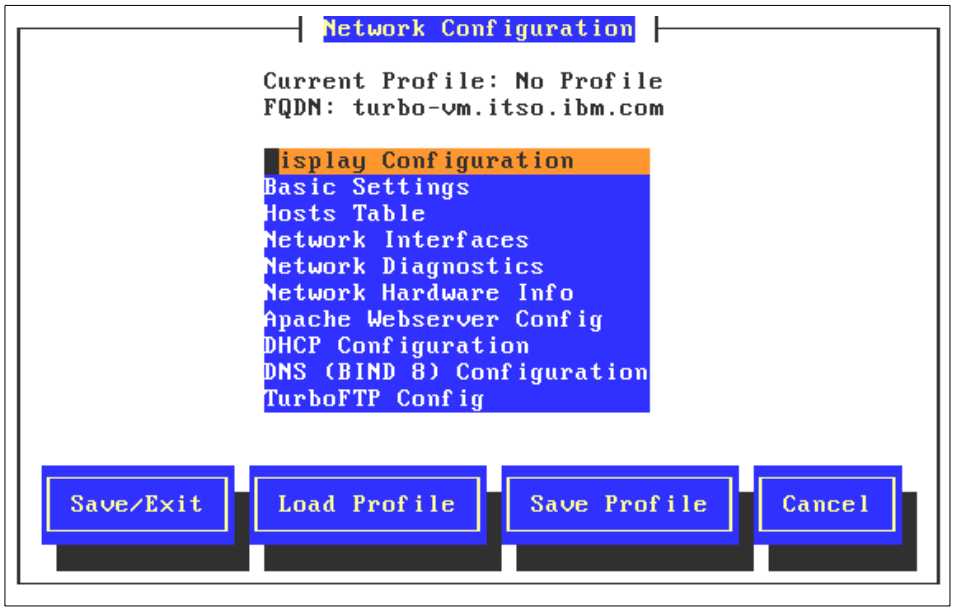


Figure 128. Main window of turbonetcfg

Figure 128 is the main window for turbonetcfg. What follows are brief explanations of all the options seen on this window.

- **Display Configuration**. Displays the current configuration of host and domain name, as well as the NICs in the machine and default router.
- **Basic Settings**. Allows you to set the host and domain name, and add search domains, secondary nameservers, and the default gateway and gateway device.
- **Hosts Table**. Used if you do not have a nameserver, or would like to specify the IP address of frequently used machines. It should also have 127.0.0.1 as localhost.It is a good idea to add your own IP and host name to this table, as it causes GNOME to start much more quickly.
- **Network Interfaces**. The network interfaces dialogue allows you to manage all the NICs in the server, including the ability to add, remove, or change interfaces without rebooting.
- **Network Diagnostics**. This is a very interesting feature of turbonetcfg. Selecting this option will cause a TurboLinux to run a series of network tests. Note that if the nameserver cannot be contacted during the “Testing Name Lookup (getbyhostname)” query. The query stays on the window for several minutes as if it has hung. However, it will eventually time out and show you a windows with the results similar to Figure 129.

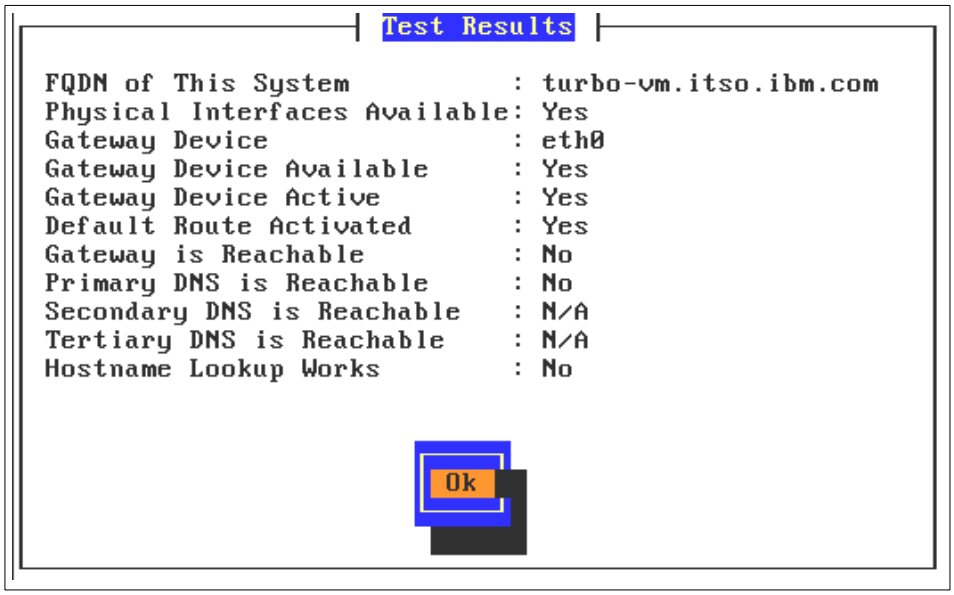


Figure 129. Test results window

- **Network Hardware Info**. This choice lists all the active interfaces and the corresponding kernel modules that support them.
- **Apache Webserver Config**. Apache is the default Web server for TurboLinux. The diagnostics allow the administrator to confirm that the server is running, as well as the current number of connections and the amount of disk space being used by /var/log/httpd.
- **DHCP Configuration**. This allows configuration of the DHCP Server.
- Note that this should be run from within X, as the configuration window requires 30 lines.
- **DNS (BIND 8) Configuration**. The TurboLinux nameserver is configured with this choice. The server can also be stopped and started here.
- **TurboFTP Config**. Configuration for the FTP server included (PROFTPD is the default FTP server). WU-FTPD is also included with TurboLinux 6, but configuration for it must be done manually.
- **IPX Config**. Allows you to activate IPX and set the IPX internal network and node number.
- **Appletalk Exports Config**. If you have MacIntosh clients in your environment, the Appletalk exports config allows you to create an Appletalk share for the network.

- **NFS Exports Config**. NFS is the traditional protocol used in UNIX environments to share files.
- **PPP Config**. This configuration tool is for the client side dialup only. It does not set up a PPP server on this machine.
- **TCP/IP Routing Config**. Allows you to set the default route and net routes. It also has an option to enable IP forwarding.

5.3 Turboprintcfg

This configuration window is identical to the print configuration window you saw during the installation of TurboLinux. We will now discuss printer configuration in more detail.

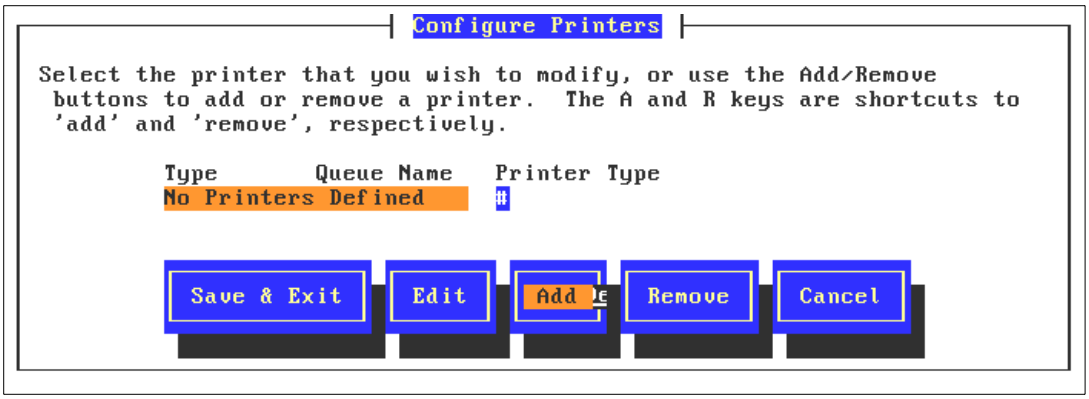


Figure 130. Configure Printers window

By selecting **Add** on the main window, you will be able to configure printers that are either local to this server, attached to another server on the network, or attached to the network directly.

5.3.1 Configuring locally attached printers

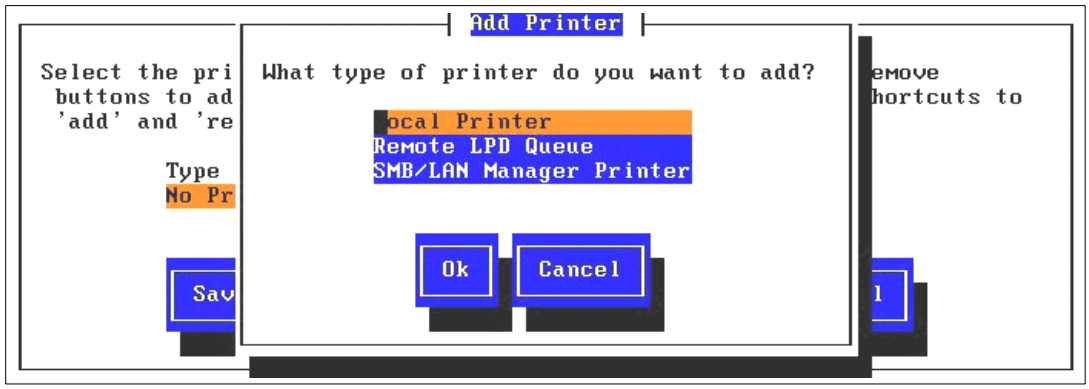


Figure 131. Add Printer window

The simplest configuration to be added is a locally attached printer. In the next figure you will see the menu displayed when **Local Printer** is selected.

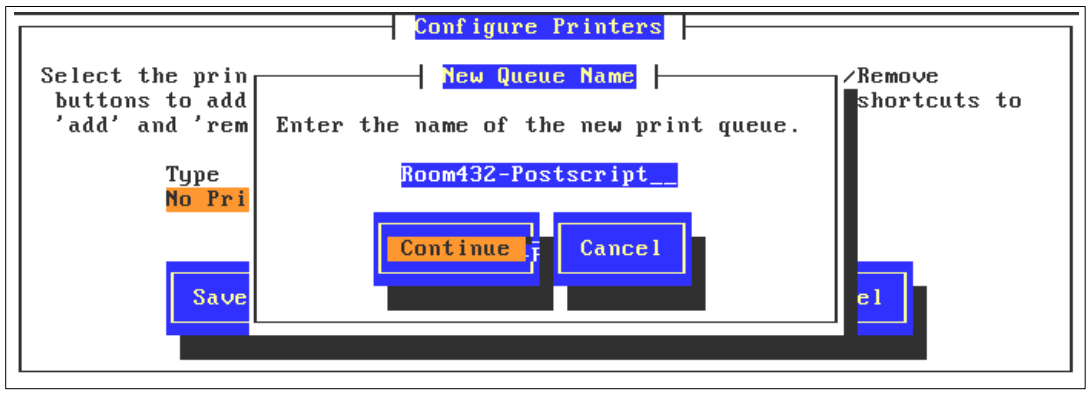


Figure 132. New Queue Name window

Above we have named the printer Room432-Postscript and selected **Continue**.

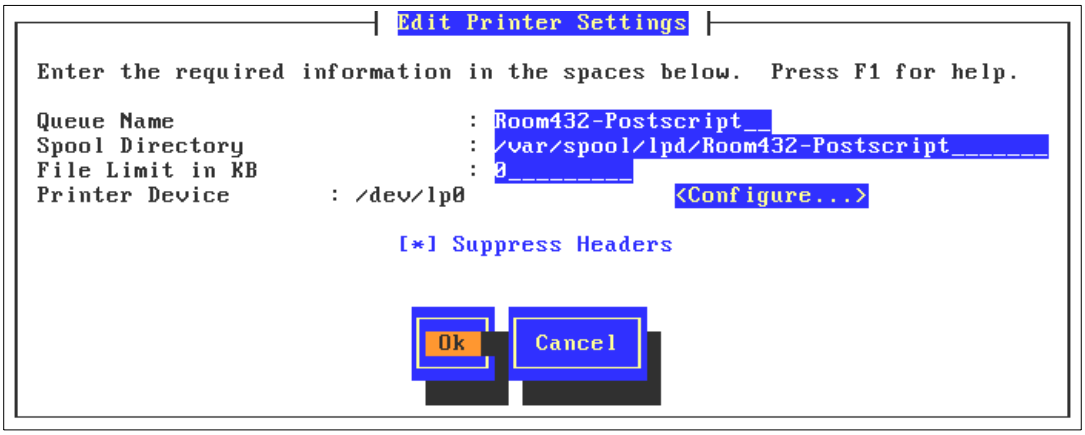


Figure 133. Edit Printer Settings window

The following information is available here:

- **Queue Name**: This will be the name users will reference when sending print jobs to this printer, whether the user is local or remote.
- **Spool Directory**: By default, Linux spools to /var/spool/lpd/[queue name]/. This can be changed if the print jobs being sent to this printer are larger than is available in the /var filesystem.
- **File Limit in KB**: This can be used to prevent large jobs from being sent to a particular printer.
- **Printer Device**: This is the output device used to access the printer.
- **Configure**: selecting this option leads to Figure 135.

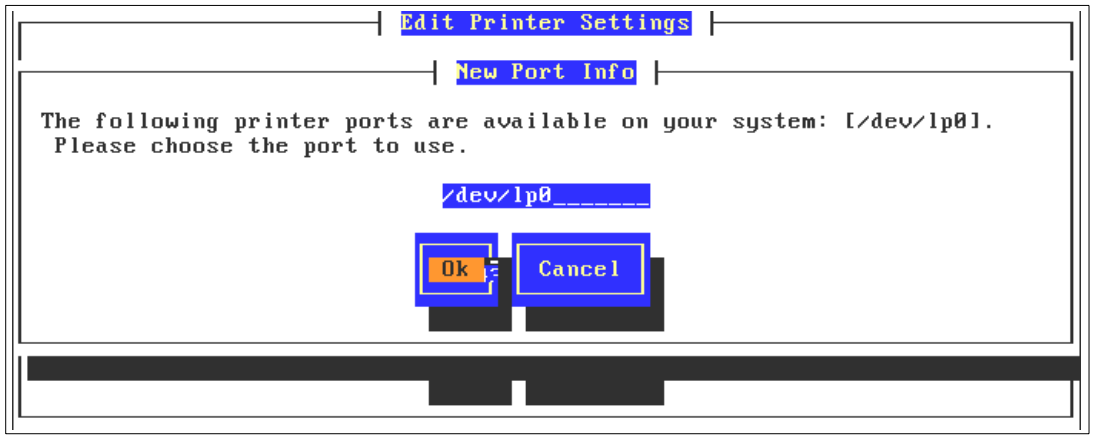


Figure 134. New Port Info window

Selecting Configure on the previous window brings up a dialog that allows you to select the output device being used to access the printer. Linux uses the convention /dev/lp0, /dev/lp1, etc. to signify what is called LPT1, LPT2, etc in Microsoft Windows. Output to serial printers is /dev/cua0, /dev/cua1, etc., to signify COM1, COM2, etc. Support for USB printers will be available in the near future when the 2.4 kernel is released. After selecting **OK**, you will return to the main window.

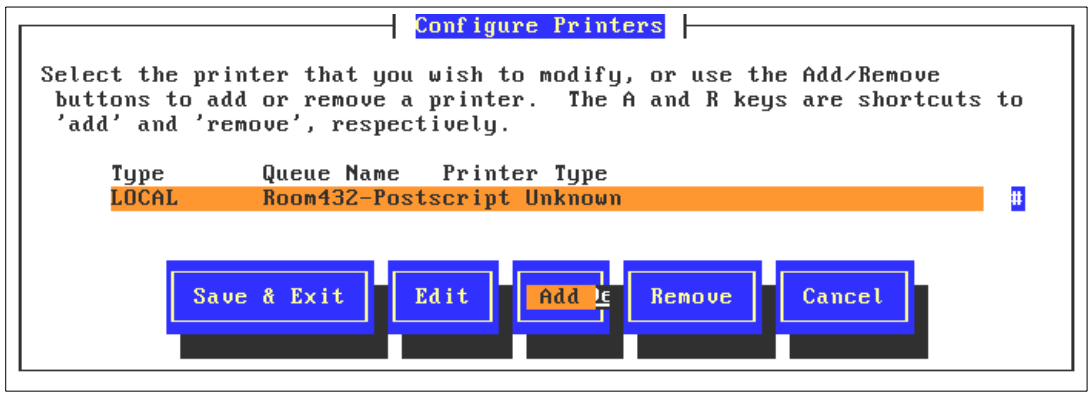


Figure 135. Configure Printers window

5.3.2 Configuring remote printers over TCP/IP

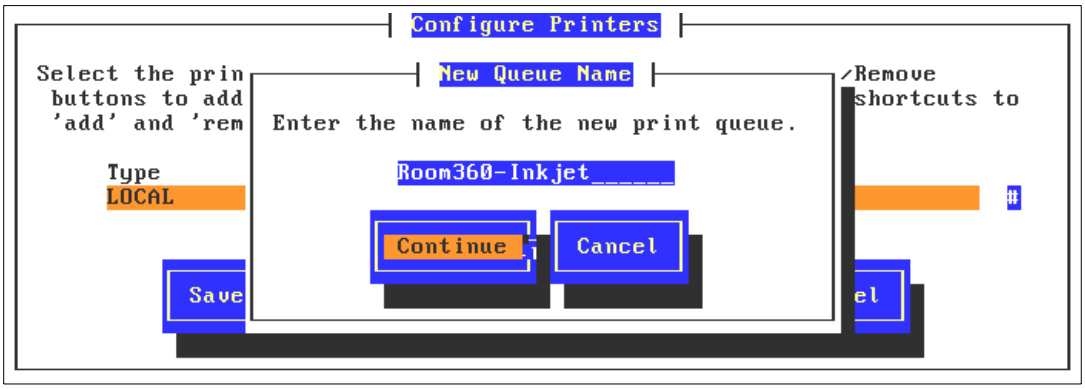


Figure 136. New Queue Name window

The process of naming a remote queue is identical to the process used for local printers. Above we have selected **Add**, then **Remote LPD Printer** and named this print queue Room360-Inkjet.

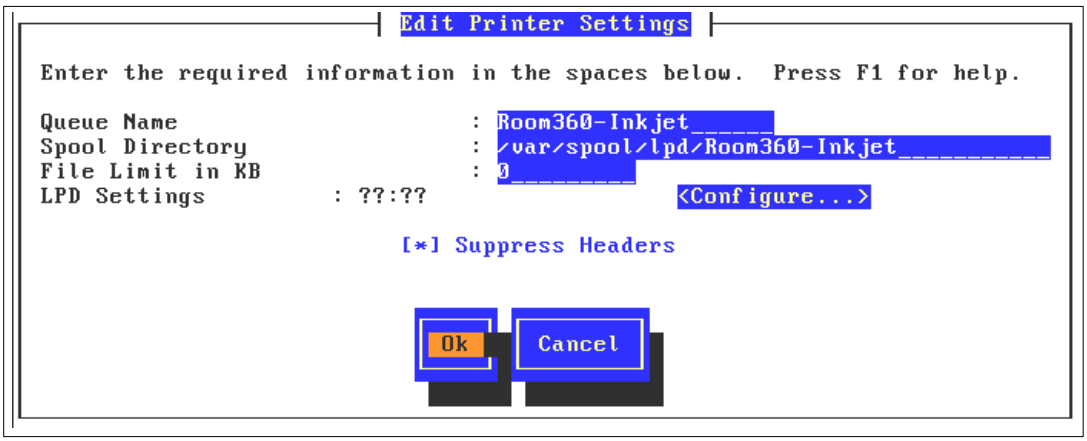


Figure 137. Edit Printer Settings window

The **Edit Printer Settings** page is also the same. Notice that **LPD Settings** is currently in the format ??:?? It is actually HOSTNAME:/QUEUE. That information is added by selecting **Configure** here.

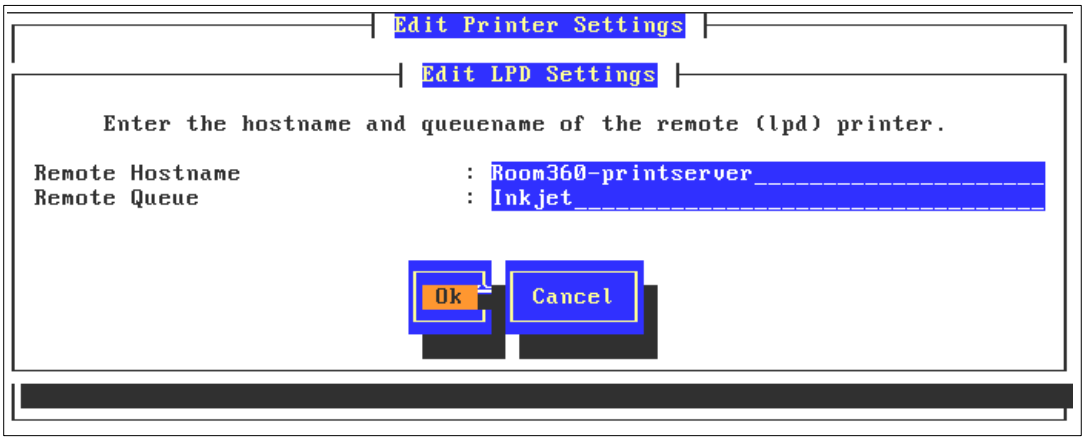


Figure 138. Edit LPD Settings window

Selecting Configure brings us to the Edit LPD Settings window (Figure 138), on which you must specify the host name and queue of the printserver you will be accessing. For LAN-attached printers that support LPD, this window will have the host name and queue defined by the printer.

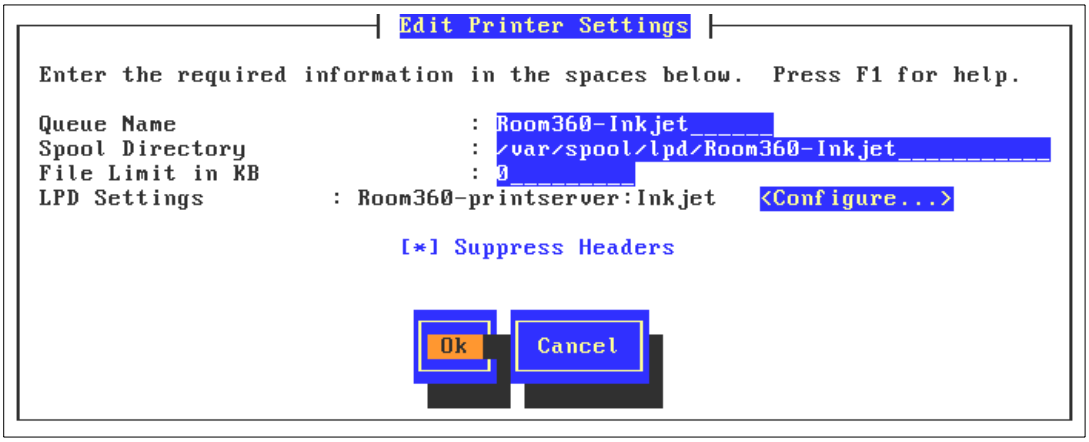


Figure 139. Edit Printer Settings window

Here you can see that LPD Settings fields now fits the pattern HOSTNAME:/QUEUE.

5.3.3 Adding NetBIOS based remote printers

Microsoft Windows and IBM OS/2 default to sharing printers over a an SMB Server Messaging Block (SMB) protocol commonly referred to as NetBIOS. If you have print shares that are accessed by SMB, you can configure Linux to act as a gateway to those print shares.

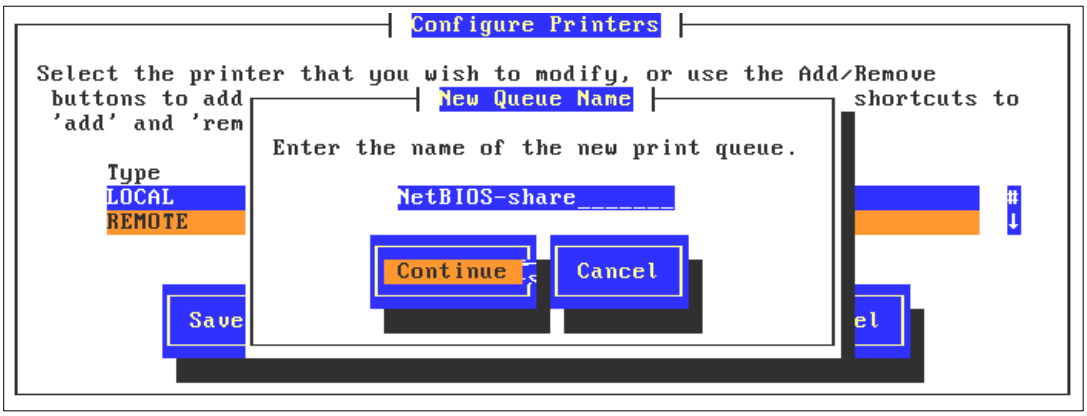


Figure 140. New Queue Name window

Above we have selected **Add** and then **SMB/LAN Manager Printer**. We have named this printer NetBIOS-share for clarity.

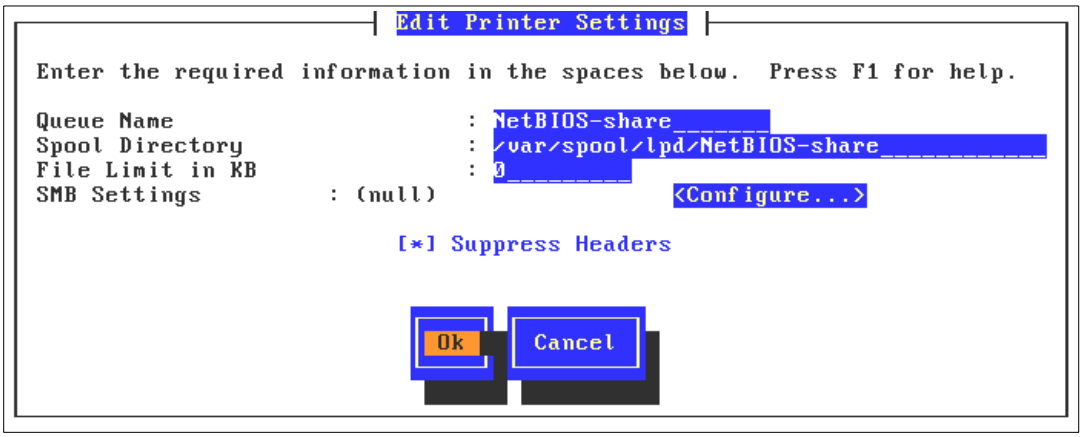


Figure 141. Edit Printer Settings window

The window in Figure 141 is identical to the window we saw in the LPD printer configuration, with the exception of the SMB Settings field. That information can be completed by selecting **Configure**.

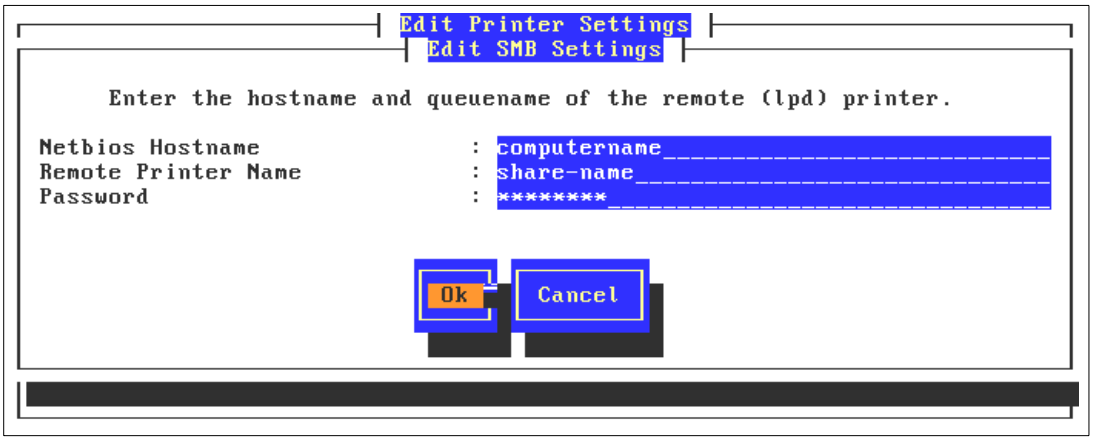


Figure 142. Edit SMB Settings window

In Figure 142 we have specified the printer settings as if it were connected to a Microsoft Windows server. NetBIOS Hostname is the Windows Computername, the Remote Printer Name is the share name in WIndows, and the Password applies if the printer is not open to everyone. Selecting **OK** then **OK** again adds the SMB printer to Linux.

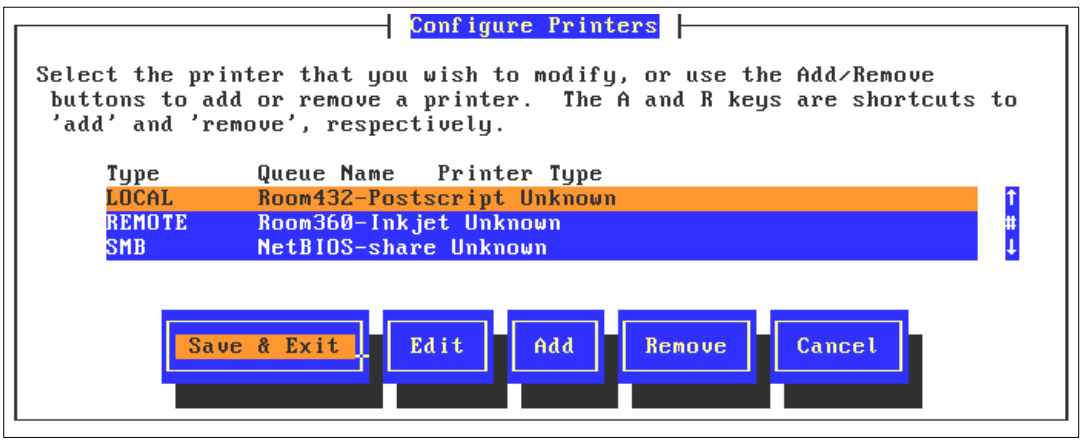


Figure 143. Configure Printers window

Selecting **Save & Exit** saves the configuration information to /etc/printcap.

5.4 Adding and removing software packages

TurboLinux uses the RPM (RedHat Package Manager) system to manage software packages. RPM uses a database to store information about the packages installed, the files that a package installs, and other relevant information needed for package management. Although several books have been written to explain all the complexity and flexibility available with RPM, we will discuss it simply as a means to easily install and remove programs.

5.4.1 Adding additional packages from the CD-ROM with Turbopkg

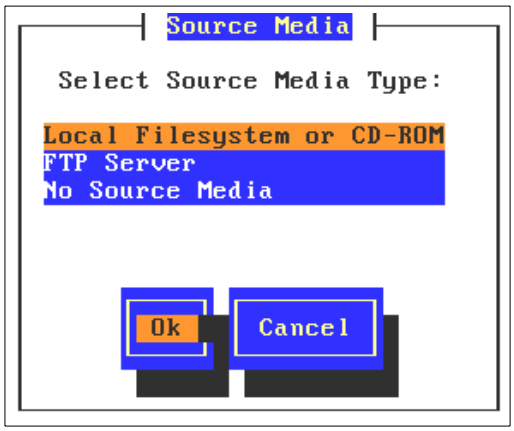


Figure 144. Source Media window

TurboLinux provides a configuration tool for the RPM system called turbopkg. Typing the command turbopkg opens the window you see in Figure 144. Here you have three options for the source of the RPMs you would like to upgrade or install. We will start by choosing **Local Filesystem or CD-ROM**.

After making the Local Filesystem or CD-ROM selection, you are presented the options of selecting User Base Path or Select Individually. Note the following information:

- **User Base Path**. This is the option you will almost always use.
- **Select Individually**. This option allows you to point to stored comp files, RPMS, and RPM header lists that do not reside in the same directory. If you choose this option, you should be aware that during a local install of packages, Turbopkg looks for three different pieces:

  a. The comps file defines the categories (for example, “Editors,’ “Basic Mail Services,” etc.) Turbopkg uses to organize all the available

packages. If the comps file does not exist, TurboLinux presents all the packages available in one long list.

b. RPMS are files that end with the extension .RPM. They contain the files to be copied, scripts to be run during or after the install, and a list other packages that are prerequisites (called dependencies).

c. RPM header files (hdlist) contain more detailed information about the RPM being installed.

In this case, we will choose **User Base Path** and proceed. This displays the window shown in Figure 145.

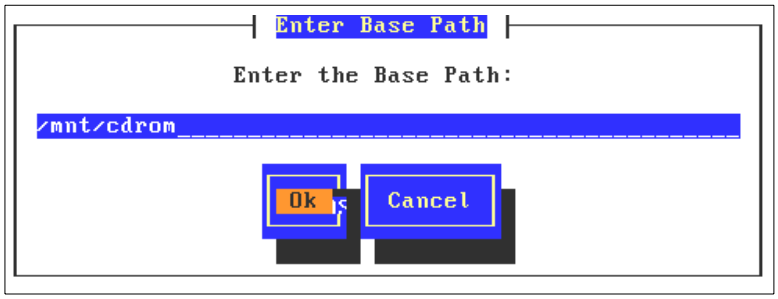


Figure 145. Enter Base Path window

Turbopkg defaults to look at your CD-ROM, but this can be changed to point anywhere. In this case we will insert the Companion CD and proceed.

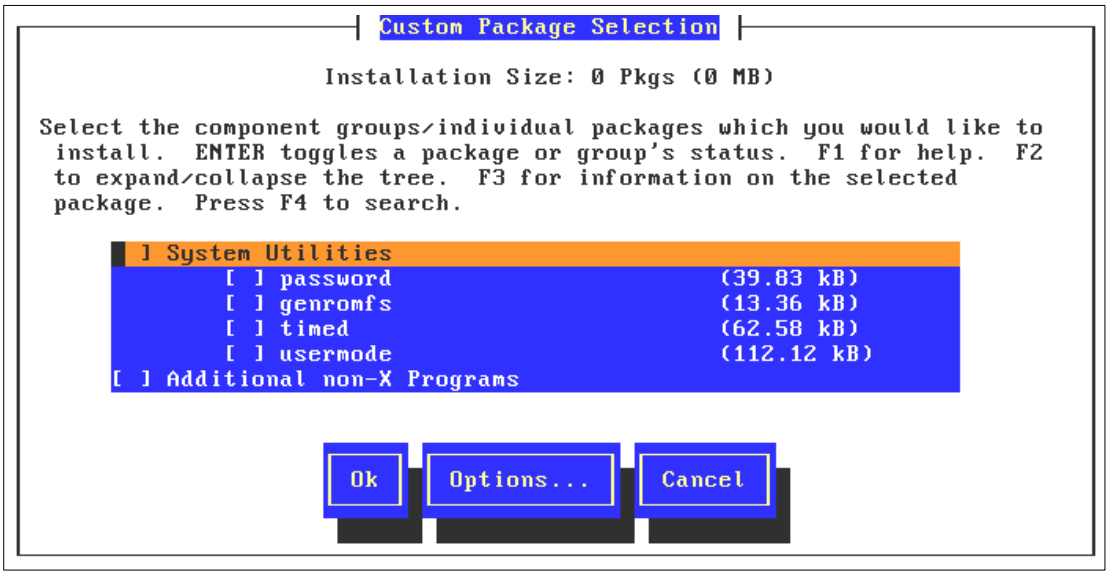


Figure 146. Custom Package Selection window

Because we selected **OK** on the previous window, turbopkg now reads the Companion CD and presents us with a list of packages to install.

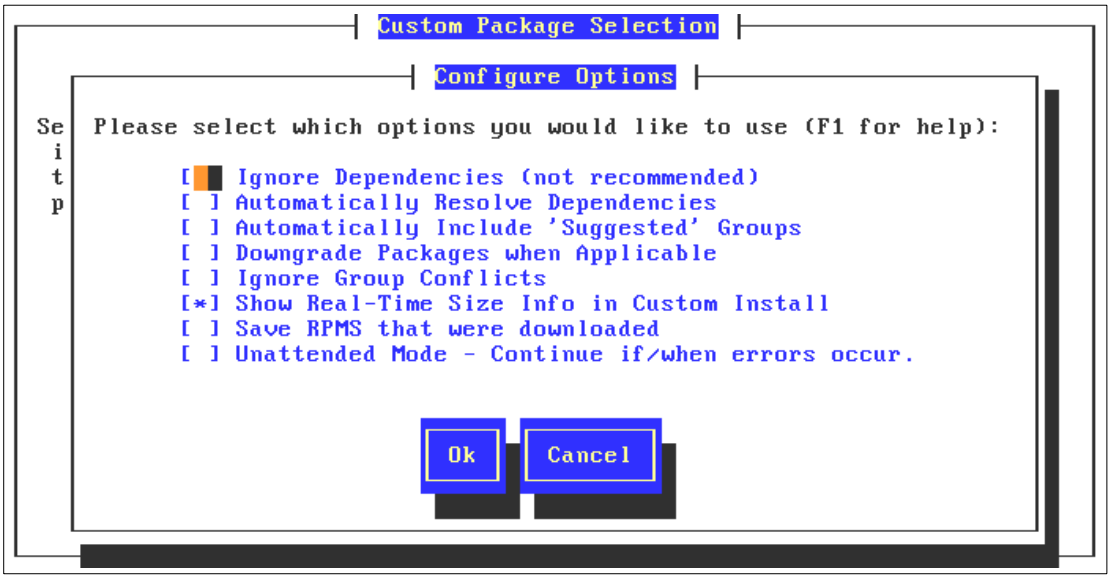


Figure 147. Configure Options window

Selecting **Options** on Figure 146 allows advanced Linux administrators to override the defaults of turbopkg. Novice and Intermediate Linux users should not change the defaults.

5.4.2 Adding packages via FTP with Turbopkg

Just as TurboLinux has the ability to install from an FTP server, Turbopkg has the ability to add new or updated packages from your own Intranet server, or publicly available Internet servers.

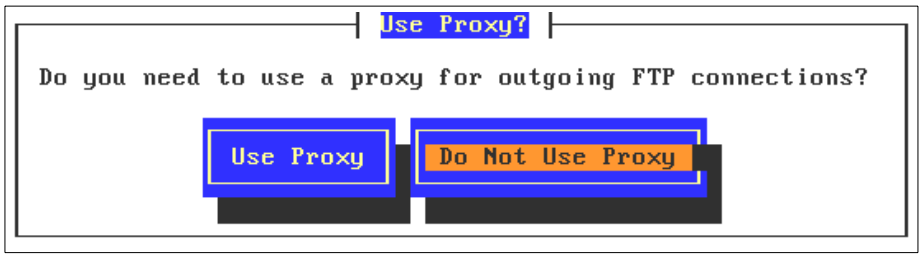


Figure 148. Use Proxy window

First we see the same dialog that appeared during the install. If your machine must pass through an FTP proxy in order to get to the server you are accessing, you must indicate that in Figure 148.

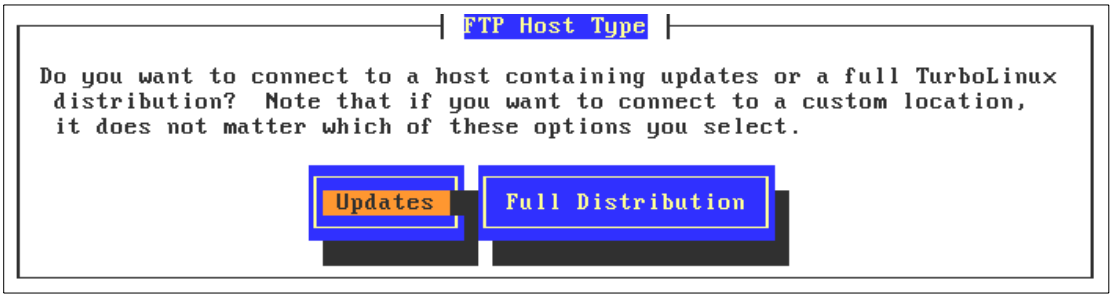


Figure 149. FTP Host Type window

We choose not to use a proxy, and since we have already completed our install, we will choose **Updates** on the window shown in Figure 149. As the text in the dialog box indicates, the option to define a custom server (for example, one within your own Intranet) will be present on the next window regardless of your choice here.

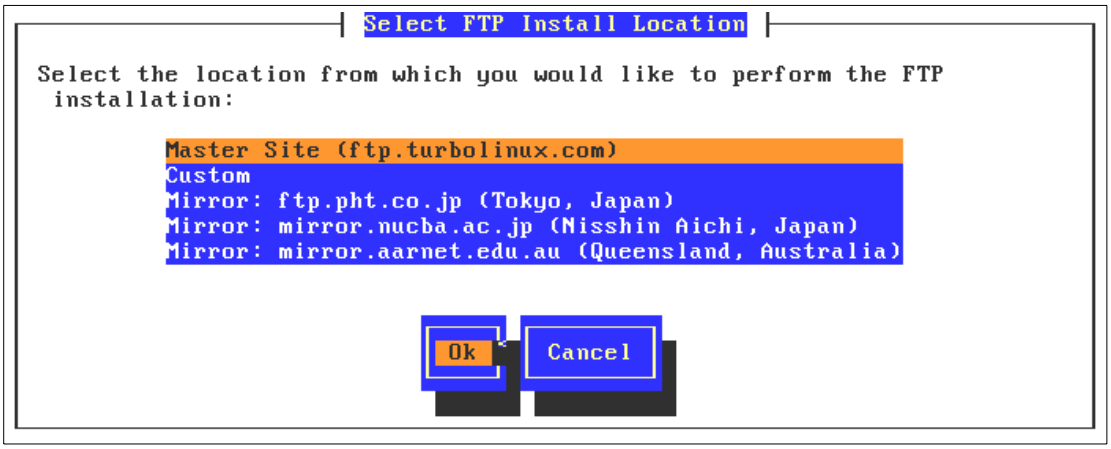


Figure 150. Select FTP Install Location window

This list of updates in Figure 150 includes both Internet sites and a Custom option, which allow you to create an update server inside your intranet. After selecting a source for the packages, the FTP method goes to the same windows we saw in the local installation.

5.4.3 Removing packages using Turbopkg

Choosing **No Source Media** in Figure 144 on page 140 takes you to the same Custom Package Selection window you have seen before. However, here your only option is to remove packages. To mark a package for removal, highlight the packages and press the key R. That will toggle the appearance of an R inside the brackets next to the package in question. Figure 151 demonstrates this.

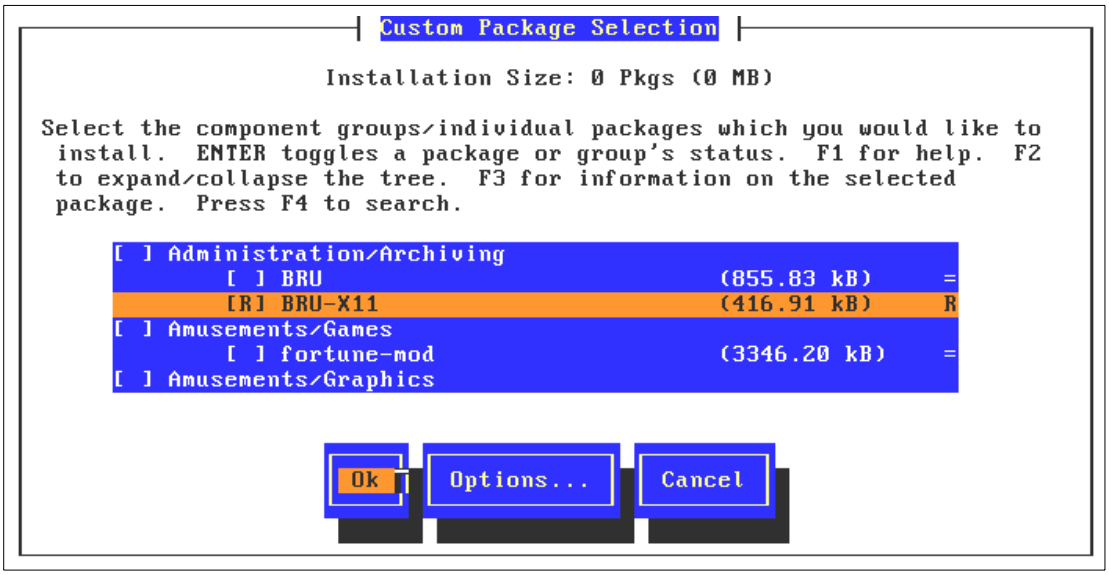


Figure 151. Custom Package Selection window

5.4.4 Package management using the RPM command

Package management can also be done directly from the command line. The command line is often used to build scripts to do package management. Table 7 table below shows some frequently used commands.

Table 7. Basic RPM commands

Command	Description
`rpm -q <package>`	Query RPM database. If package is installed, display version and build number of installed package.
`rpm -qi <package>`	Obtain some more information about an installed package.
`rpm -qa`	List all installed packages.
`rpm -qf <filename>`	Determine the (installed) package that `<filename>` belongs to.
`rpm -Uhv <package.rpm>`	Update/Install the file `<package.rpm>` showing a progress bar.
`rpm -F -v ./*.rpm`	Update (refresh) all currently installed packages using the RPM files in the current directory.

Command	Description
`rpm -e <package>`	Erase or remove a package

More information about RPM can be found in the manual page (man rpm), the RPM HOWTO or the RPM Web site at `http://www.rpm.org`. You can also display a short overview by running `rpm --help`.

5.5 User and group administration

Linux is a multi-user operating system. To differentiate between the various users, each user has to log in with a unique user name and password. Each user belongs to a primary user group, but he can also be a member of additional other groups as well (up to 16 groups). Each user name is assigned a numeric identifier called a UID (User Identifier) which is unique throughout the system. Groups also have a numeric identifier, called a GID (Group Identifier), that is unique to the system as well. For environments where security is handled by individual machines, this can be important, since some services rely on the UID and GID to determine permissions. Those issues can be resolved by using NIS (Network Information Service) or LDAP (Lightweight Directory Access Protocol), but for now we will put those questions aside and look at the menu system TurboLinux provides for managing groups and users on individual machines.

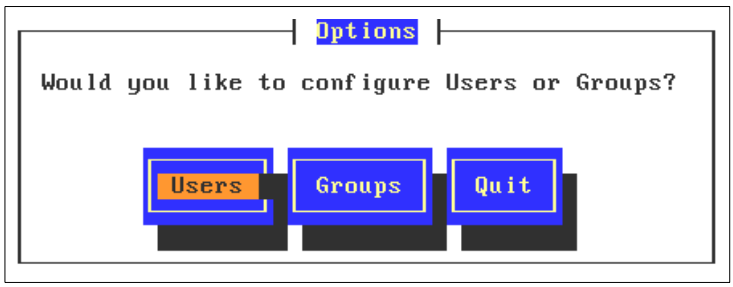


Figure 152. Options window

Issuing the command `turbousercfg` creates the window shown in Figure 152. On it you have the ability to manage both **Users** and **Groups**.

5.5.1 Adding new groups

You should consider adding groups before adding users. Sometimes there are concerns about restricting access to some parts of the user file system. You can do this by creating separate user groups to control access to various

files and file systems. Also if you are going to be creating a system with many users, you should consider creating separate groups divided by what they are doing on the system. You can create an admin group for admins, a db2user group for DB2 users, and so forth. Linux allows you to control access to both files and directories by users, groups, and everyone on the system.

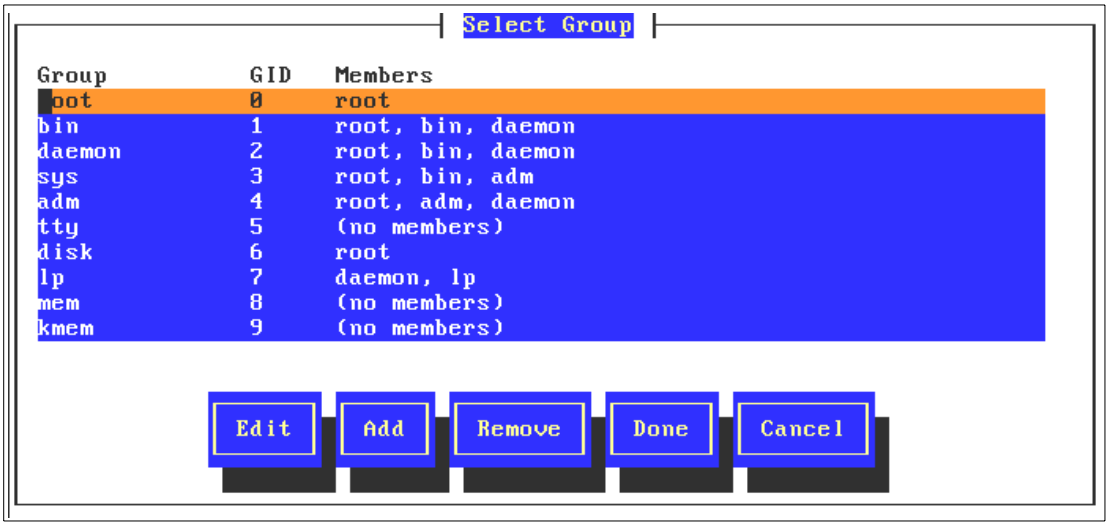


Figure 153. Select Group window

Selecting **Groups** creates the menu you see Figure 153, which is a partial listing of the default groups created by a complete install of TurboLinux. This is a very long list, and if you scroll through you will get some feeling for the different groups that can be created. The list of groups is stored in the file /etc/group.

The information that is displayed is:

- **Group.** This is the unique name of the group.
- **GID**. The system knows a user and group only by a number. In this case the group is known by the group ID. The group ID must be unique.
- **Members**. This is a list of the members of the group.

You should also notice that you have the option to select:

- **Edit** a current group listing. This allows you to change characteristics of groups that are on the list.
- **Add** a new group.
- **Remove** a current group.

- **Done**. This allows you to save any changes you have made.
- **Cancel**. This allows you to back out of any changes that have not been saved.

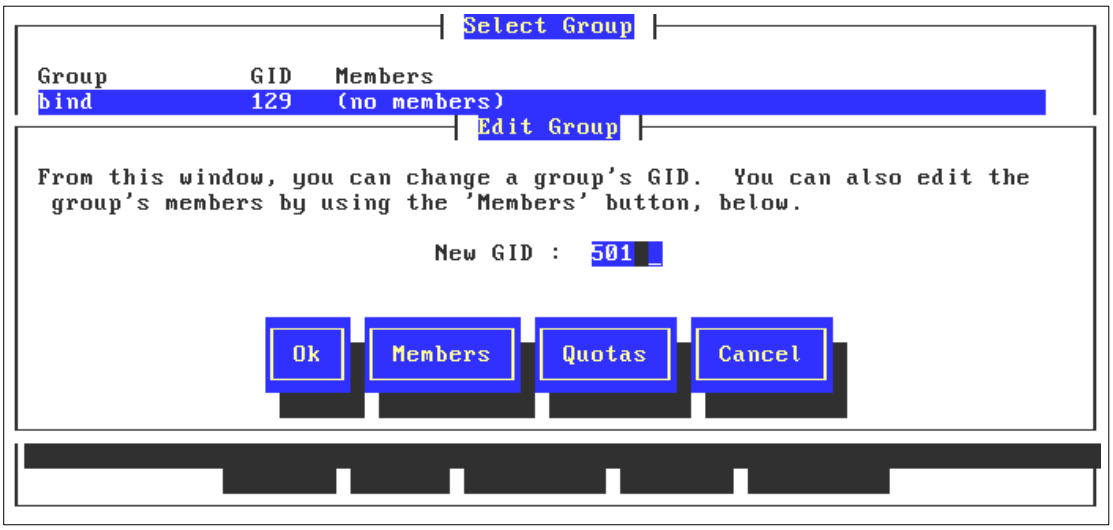


Figure 154. Select Group window

If you decide to Add a group you will first see a window that asks you to name the group, and will then see the window in Figure 154. Here you can change the GID for the group, as well as add and remove Members (users) from the group. If you have disk Quotas enabled, you can set quotas for the group as well.

5.5.2 Adding new users

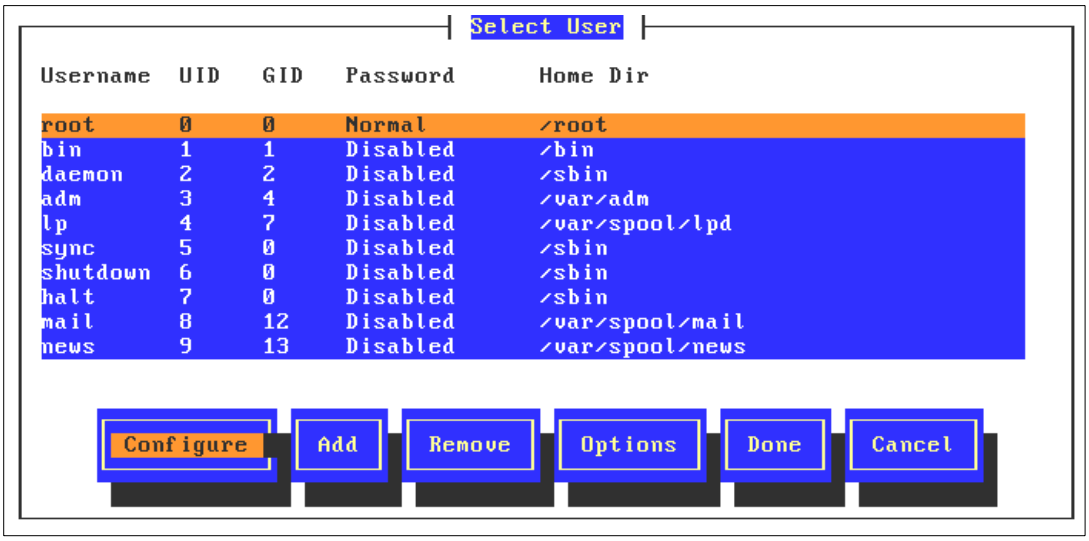


Figure 155. Select User window

Above you see a human readable form of the user information stored in the file /etc/passwd.

The information in Figure 155 is organized in columns by:

- **Username.** This is the unique name that a user types at the login prompt. It can also be called the login name, ID, user login, user, or user account.
- **UID**. This is the number that the system uses to identify each user. Each user on a particular system has a unique UID.
- **GID**. This is the unique number assigned to a group. Every user has a default group. In TurboLinux the default GID is 100.
- **Password**. This does not contain the password but tells you the information about its state. The column is either:
  - **Shadowed**. Which means it is using the shadow password file to store the password instead of /etc/passwd.
  - **Disabled**. The account is disabled, or is a service. Services are assigned a UID but no password, as they do not log in in the same way human users do.
  - **Home Dir**. This is the user's home directory. It is the first place a user goes when logging in. It contains files and programs that are owned and used by that user.

In addition there are several choices for adding or configuring users that are given to you in the boxes along the bottom. They are:

- **Configure**. This allows you to change the characteristics that were set up when the ID was created.
- **Add**. Allows you to add users, which will be discussed later.
- **Remove**. Allows you to remove the user. You can optionally also remove the home directory.
- **Options**. Allows you to configure options for the user such as file system space quotas if they have been enabled.
- **Done**. Will allow you to quit and will save any unsaved information.
- **Cancel**. Will allow you to quit and *not* save any information.

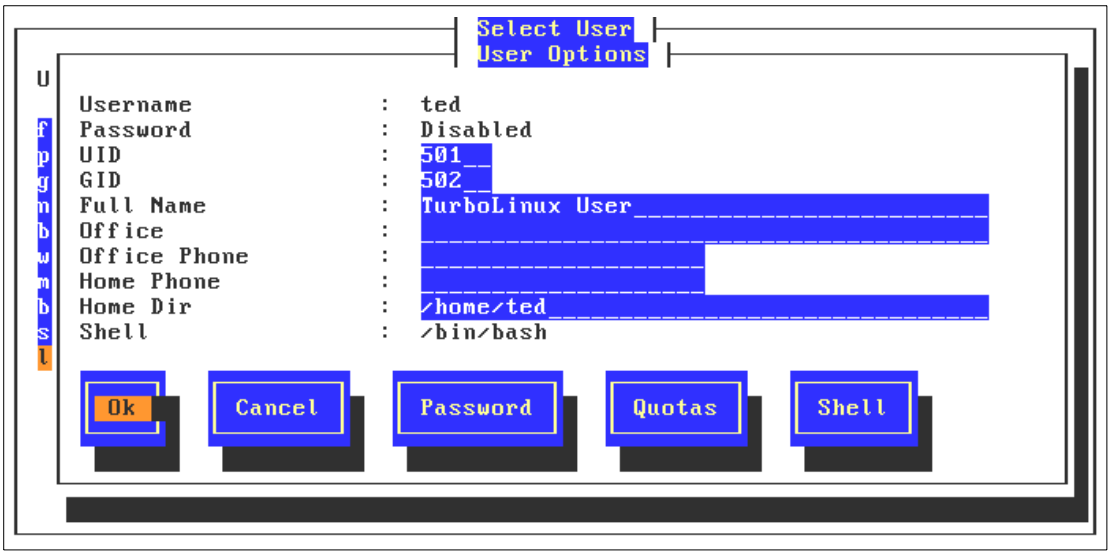


Figure 156. User Options window

To add a user select the **Add** option at the bottom of the window. You will then see a window asking you to give the name of the new user, and specify the home directory for this user. We recommend you accept the default location of /home/<username>/.

You will then come to the window Figure 156. The information that can be added for each user includes:

- UID
- GID

- Full Name
- Office
- Office Phone
- Home Phone
- Home Dir

The buttons at the bottom of the window allow you to modify the following:

- **Passwords** must be at least 4 characters long.
- Disk **Quotas** can be defined per users if you have file systems on this server that have quotas enabled.
- The default **Shell**, bash, will suffice for almost all users. On occasion, some users may prefer a different shell. You can set the user's default shell here.

Here is a brief description of the included shells:

- **/bin/bash**. This is the Bourne Again Shell, which is an extension to the Bourne Shell. This is the most popular shell for Linux.
- **/bin/sh**. This is the standard Bourne Shell that has been around since almost the beginning of UNIX.
- **/bin/ash**. This is another version of the Bourne Shell.
- **/bin/bsh**. This is the same as /bin/ash to which it is linked.
- **/bin/ksh**. This is the standard Korn Shell that is the most popular shell for UNIX administration.
- **/bin/tcsh**. This is a public domain extension of the C Shell.
- **/bin/csh**. This is the standard C Shell that was originated by the University of California at Berkeley.
- **/bin/zsh**. This is another extension of the Bourne Shell.

Your choice of shells is strictly a matter of preference, but generally UNIX admins prefer Bourne or Korn Shell programs, whereas programmers tend to prefer C Shell-based programs.

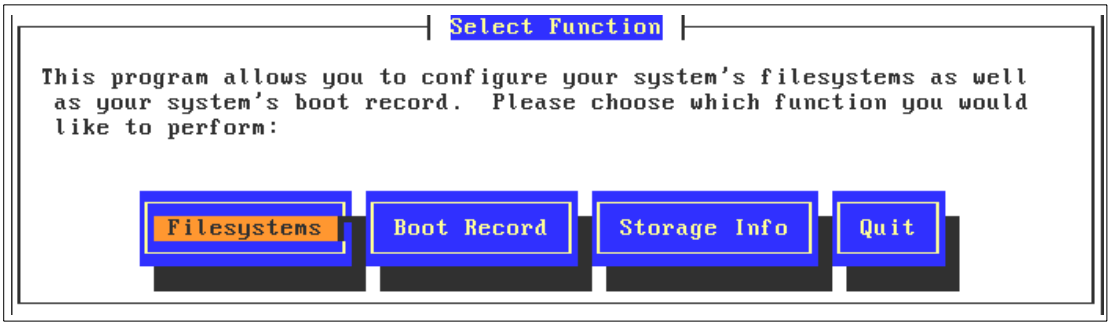


Figure 157. Select Function window

Running the command `turbofscfg` generates the menu you see Figure 157. From here the administrator can manage almost all issues that touch the DASD attached to this system. To view all the DASD Linux sees on your server, select the option **Storage Info**. That will display a window similar to Figure 158.

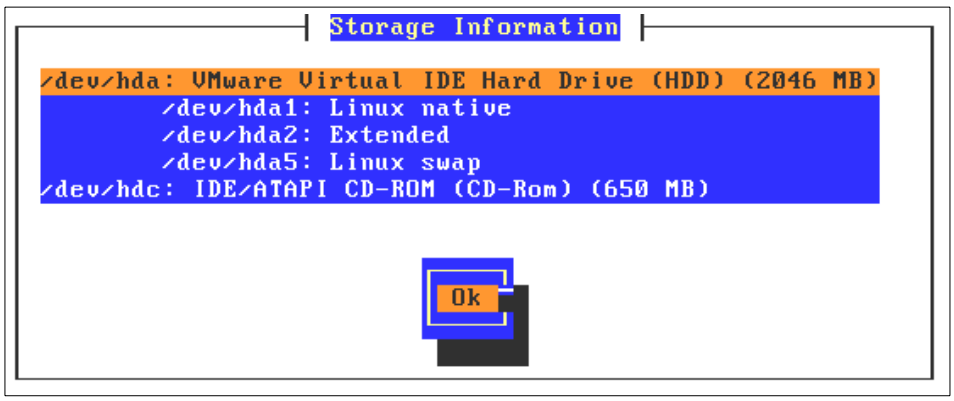


Figure 158. Storage Information window

Notice that in the example above, the mounted CD-ROM appeared as well.

5.6.1 Managing file systems

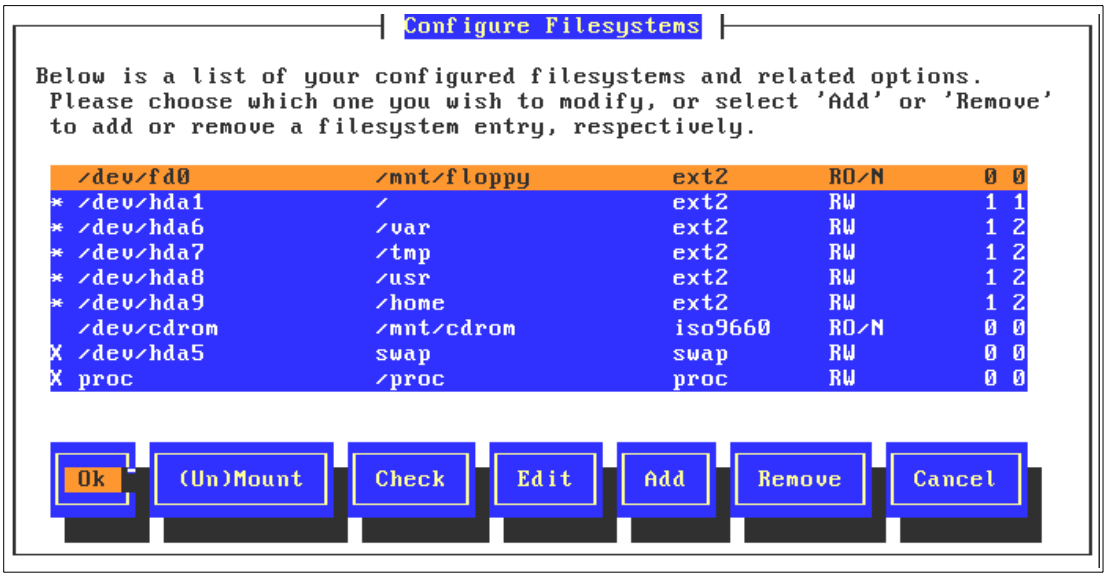


Figure 159. Configure Filesystems window

Above you see the main window created when the Filesystems option is selected from the main turbofscfg window. The columns of information displayed (which is being read from /etc/fstab) are from left to right:

- **Mount status** is indicated by an * for mounted file systems and a blank space for unmounted file systems. In the figure above the floppy and CD-ROM are not mounted.
- **Device**, which is where raw device exists in the file system. This is how the kernel sees the device.
- **Mount Point**. Linux uses a concept of mount points to give the user access to DASD devices. This allows you as the user to map an arbitrary name to a fixed name that is known to the kernel. So, for example, if you wanted the TruboLinux 6 CD-ROM to be accessible to FTP users, you could mount the device /dev/cdrom to /home/ftp/pub/TurboLinux6. This column lists the mount points currently assigned to the filesystem table.
- **Default filesystem Type**. When a device mounts, it mounts with the file-system in this column. Notice that the floppy drive defaults to ext2, which is actually rather rare. To mount FAT-formatted floppies, you will need to change the file system type to MSDOS. That example is given at step 3. on page 154 when we discuss the **Edit** option.

- **Permissions**. Whether the file system is readable and/or writable.
- **FSCK options**. These two numbers determine whether the file system should be dumped if the system crashes (0 for no, 1 for yes), and the priority FSCK should use when running (0 indicates the file system should not be checked, 1 indicates that FSCK should check this file system first, 2 indicates that FSCK should check after all the file systems numbered 1 have been completed.

In addition to the columns of information, there are several options at the bottom of the window. We now address them:

1. **(Un)Mount** toggles the mount status of file systems. With this option you can mount filesystems that are currently mounted, and unmount nonessential mounted filesystems.
2. **Check** allows you to force FSCK to run now. You can only run FSCK against unmounted filesystems.
3. **Edit** allows you to change various attributes of the mount point. For example, the window below was generated by highlighting the first line in the table (the floppy drive) and choosing **Edit**. In the next few windows, we show you how to change the default file system to MSDOS.

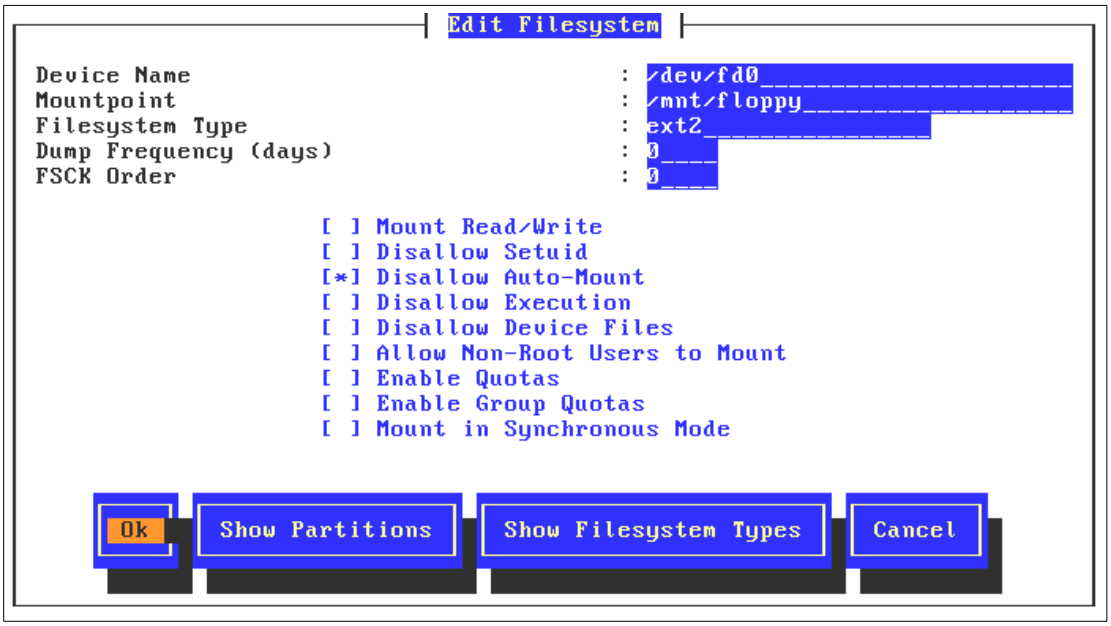


Figure 160. Edit Filesystem window

You can see in Figure 160 that the Filesystem Type is set to ext2. Selecting **Show Filesystem Types** allows you to view the other available options in the Figure 161.

Figure 161. Filesystems window

The DOS filesystem FAT is referred to by Linux as MSDOS, and we can see from this list that it is available. Note that this list is a real-time listing of all kernel modules in the directory /lib/modules/current/fs/. If modules are removed or added to the directory, the list will change.

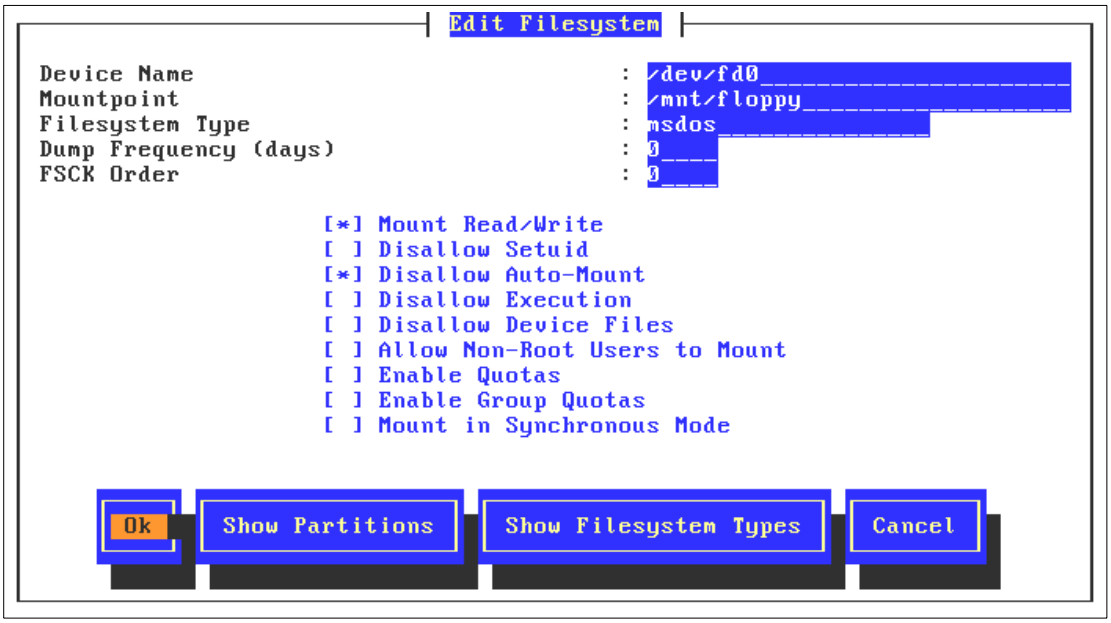


Figure 162. Edit Filesystem window

In Figure 162 we have changed the Filesystem Type to msdos, and selected the option to mount the floppy read-write, since a read-only floppy is not very useful. Clicking **OK** on this window saves our changes to /etc/fstab.

4. You are allowed to add local or remote file systems to this server. Selecting Add will give you the options shown in Figure 163:

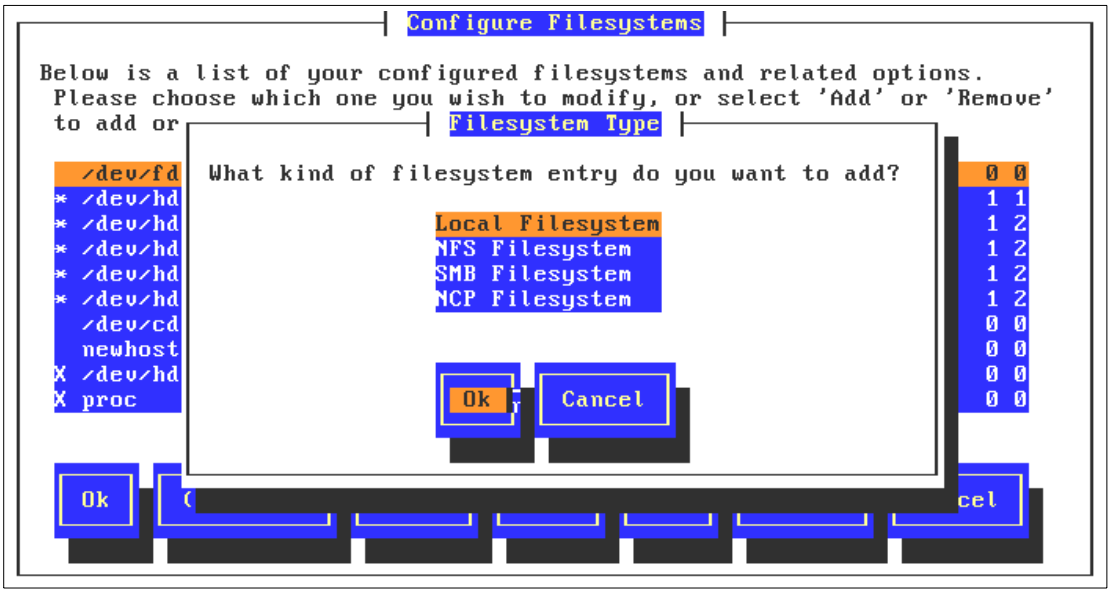


Figure 163. Configure Filesystems window

The four types of filesystems that can be added are:

a. **Local Filesystem**. This window is identical to the Edit Filesystem window shown in Figure 163. When adding a file system, the options Show Partitions, and Show Filesystem Types are quite helpful, as they allow you to view all the partitions and file systems known to the system.

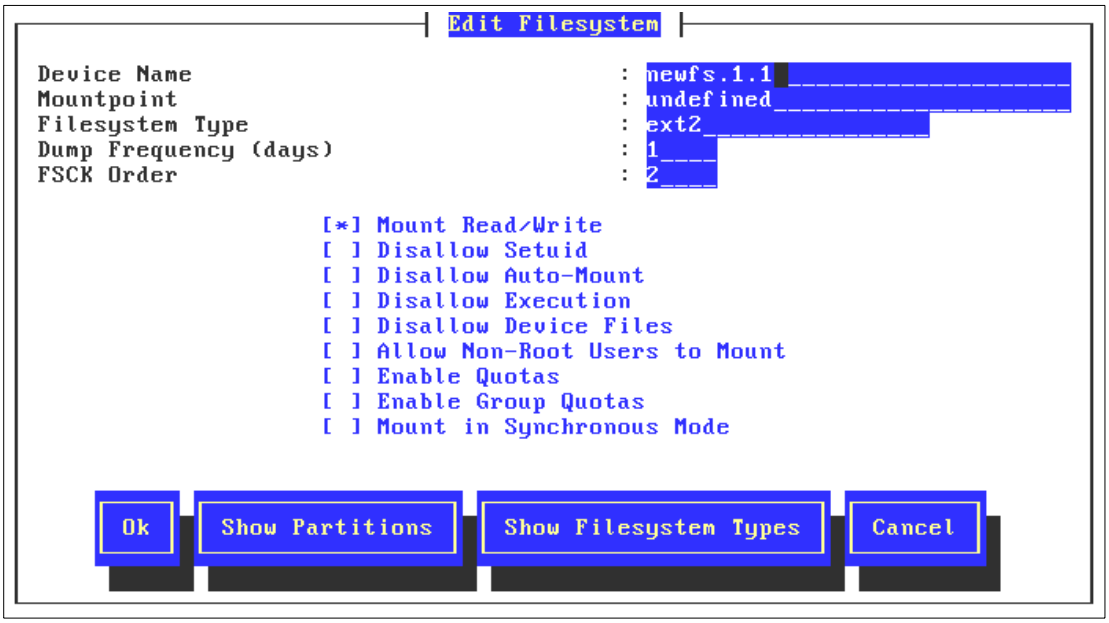


Figure 164. Edit Filesystem window

b. **NFS Filesystem**. This options allows you to mount filesystems being exported by an NFS server. You can get a list of the directories being shared by a server by completing the first line, Hostname of IP Address and selecting the option **NFS Exports**. That will query the NFS server in question and send back a list of directories being exported (also called exports).

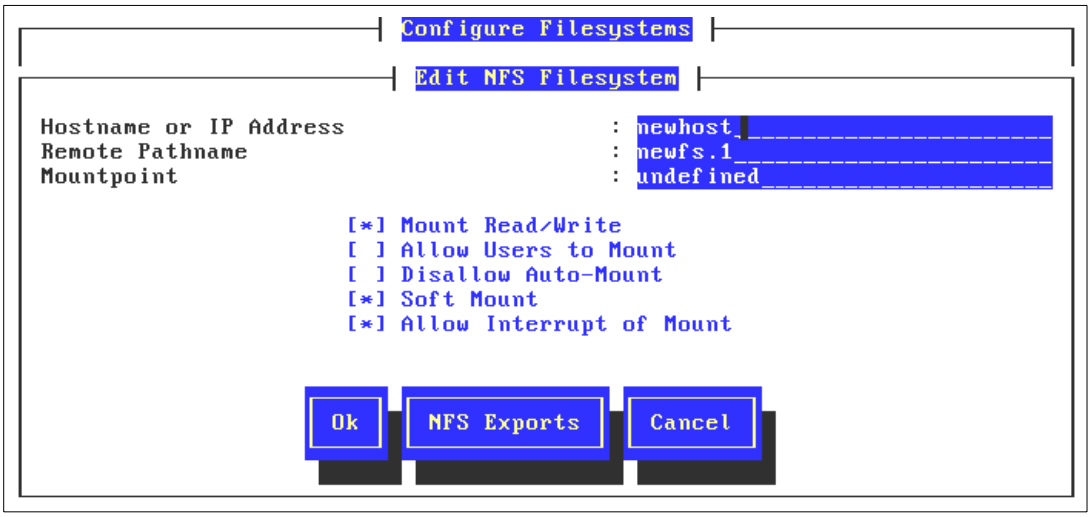


Figure 165. Edit NFS Filesystem window

c. **SMB Filesystems** are the NetBIOS shares offered by Microsoft Windows and IBM OS/2 servers. Enter the server's NetBIOS Name and select the **SMB Shares** option shows the shares being offered by the SMB server.

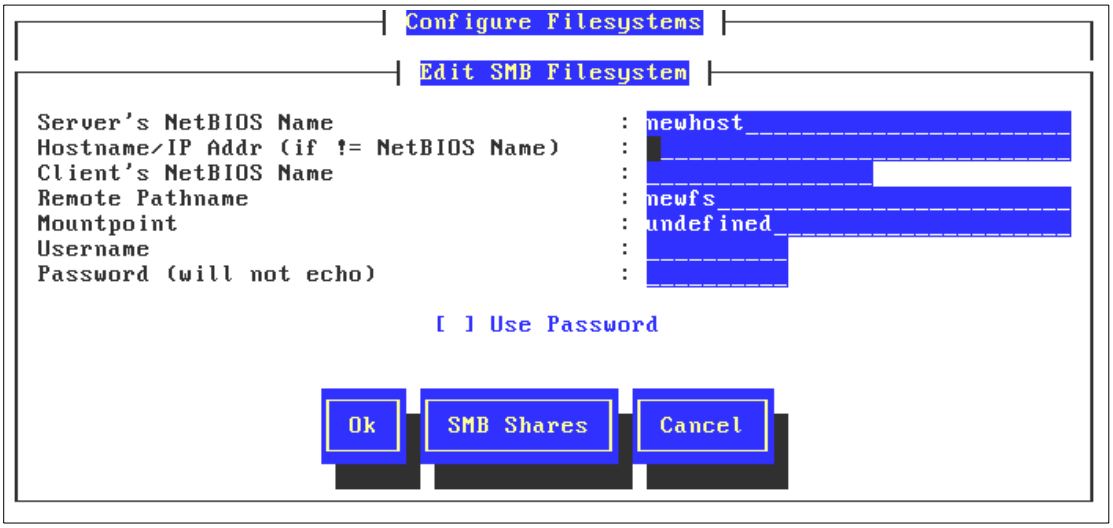


Figure 166. Edit SMB Filesystem window

d. **NCP Filesystem** offered by Novell NetWare servers can be added by choosing the last option.

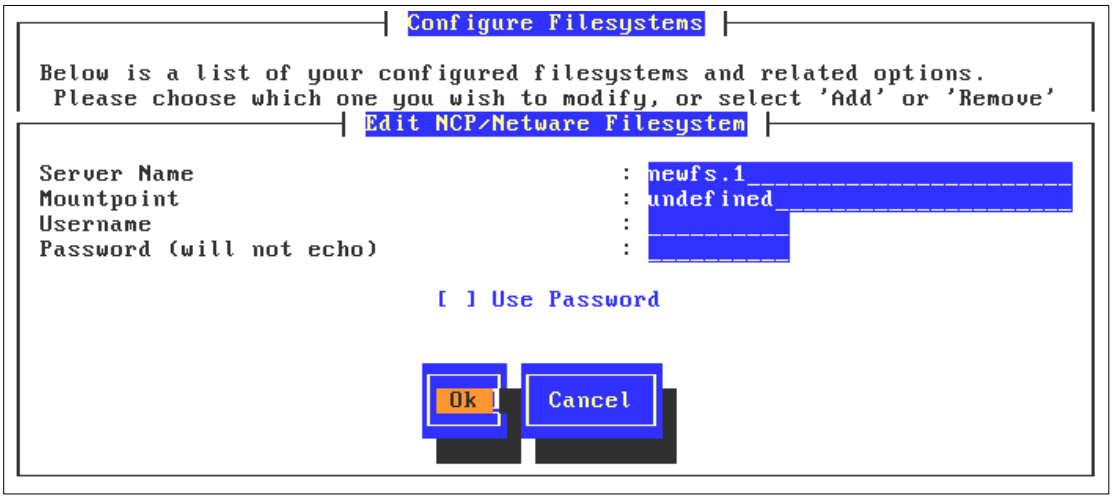


Figure 167. Edit NCP/NetWare Filesystem window

5.6.2 The Boot Record

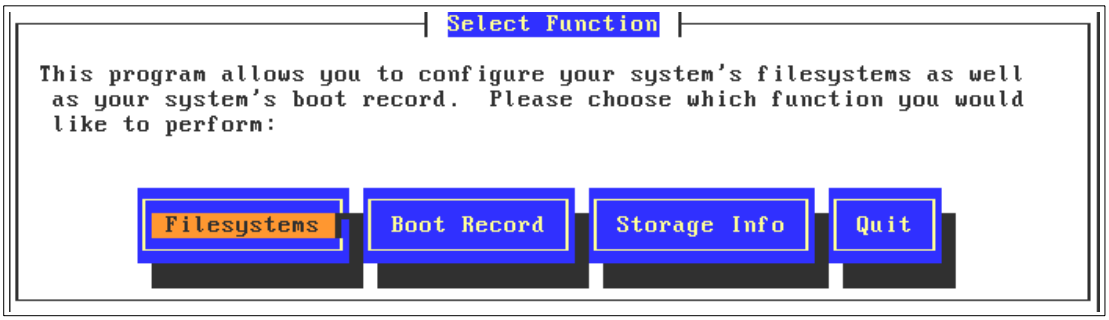


Figure 168. Select Function window

When Linux is installed, it is the responsibility of the program LILO to write the correct information to the Master Boot Record and Boot Record of the computer so Linux can boot. In Figure 168 you see the main window for turbofscfg again. Choose **Boot Record** here and proceed.

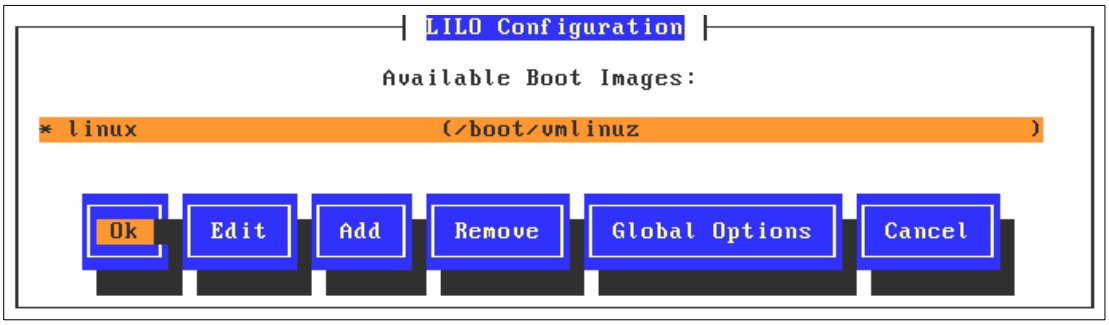


Figure 169. LILO Configuration window

Choosing Boot Record on the main turbofscfg window brings you to Figure 169. By default, TurboLinux creates a boot image labeled “linux” that boots the kernel /boot/vmlinux. The * on the left side denotes that this is the default image to boot if there are multiple images. The other options on this window are:

1. **Edit**, which allows you to change the configuration of an image. Below you see the details for the default “linux” configuration.

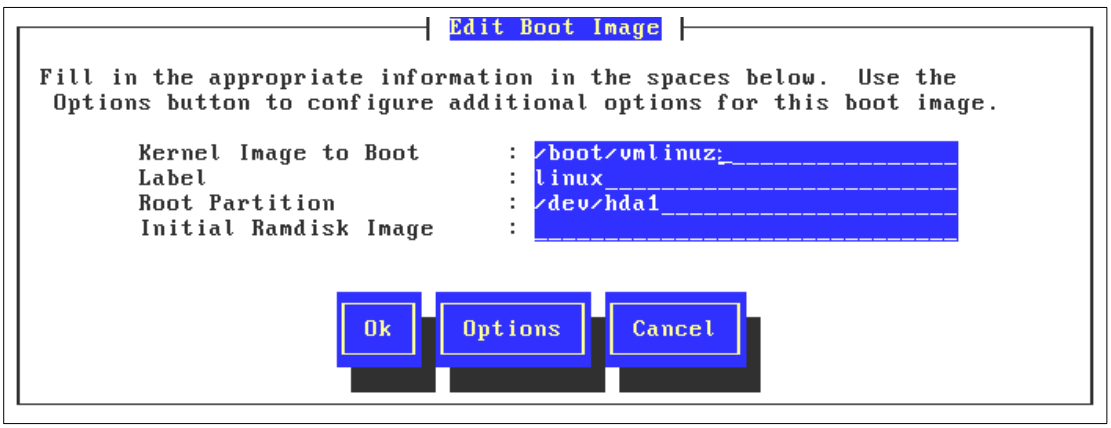


Figure 170. Edit Boot Image window

2. **Add**, which allows you to create a configuration for a different Linux kernel, or a different operating system on a different partition. When you choose Add, you will be asked if you would like to add a Linux or non-Linux boot image. Adding a Linux partition generates the same window you see in Figure 170. Choosing to create an image for a non-Linux operating system creates the following window:

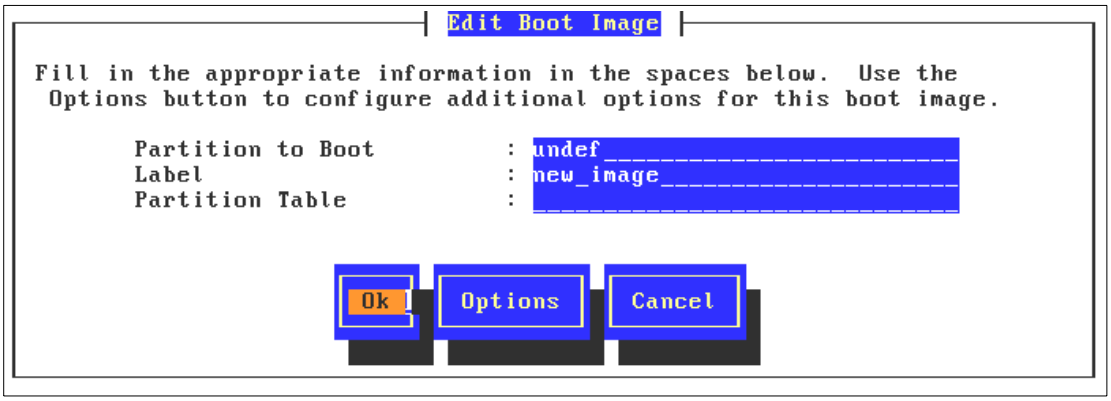


Figure 171. Edit Boot Image window

Here you define the partition you would like to boot. The partitions are defined as Linux sees them, so /dev/sda and /dev/sdb are the first and second SCSI drives, and /dev/hda and /dev/hdb are the first and second IDE drives.

3. **Remove** will erase the entry from /etc/fstab.
4. **Global Options** sets many other LILO options.

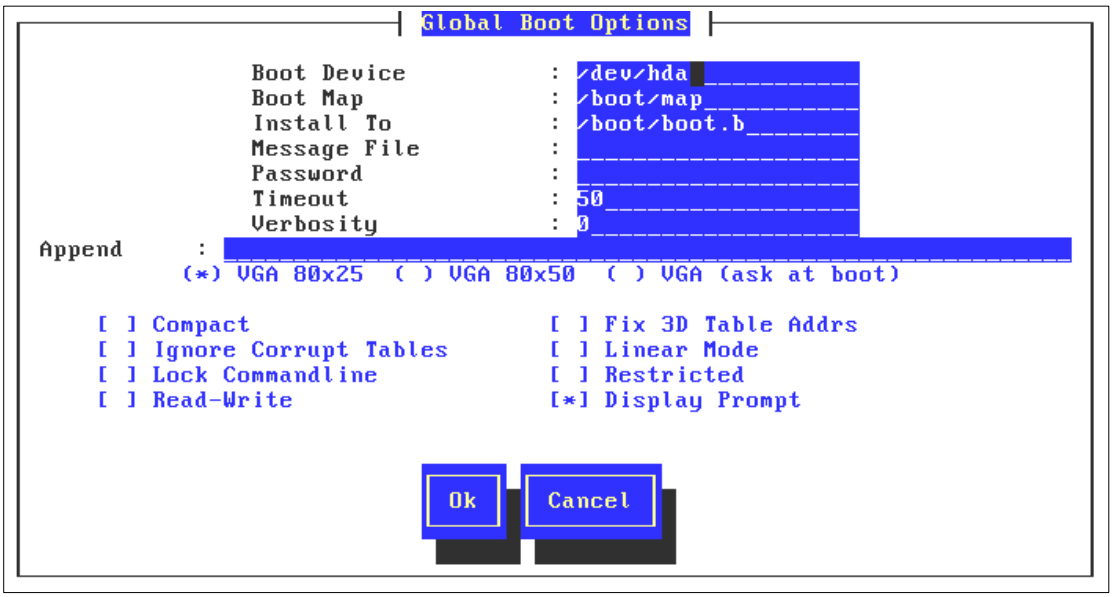


Figure 172. Global Boot Options window

Those options are:

- **Boot Device**. The hard drive on which LILO will write its information, and the choice of using the either Master Boot Record (in this case /dev/hda) or the boot record of a partition (for example, /dev/hda1). You can write LILO to a partition if you would like some other boot loader program to control the Master Boot Record.
- **Boot Map** and **Install To** are internal configurations of LILO, and should not be changed.
- **Message** allows you to insert a message that is seen when LILO starts.
- **Password** allows you to add a password to LILO.
- **Timeout** is time in seconds before the default boot image is executed.
- **Verbosity** defines the amount of information LILO gives to the administrator when it is writing to the drive. The scale is from a low of 0 to a high of 5, and the information is only shown if the LILO command is issued from a command line. You will not see any additional information if you use turbofscfg.
- **Append** allows you to add extra parameters to the kernel. Some configurations may need extra parameters to start certain devices.
- **VGA** resolution choices are 80x25 or 80x50, or you can require the choice to be made at boot time. Note that “ask at boot” offers a few other resolution choices.

The other options on this window are beyond the scope of this book. If you need more information on them you can read the LILO HOWTO at

`http://www.linuxdoc.org/HOWTO/mini/LILO.html`

5.7 Determining your hardware

There are several ways you can determine your hardware. These methods include:

- **Bootup messages**. The file /var/log/messages is a plain text file containing the bootup messages. The system will attempt to find hardware devices when you boot up. It may recognize the hardware devices and then attempt to use modules that are compiled in the kernel or modules that are loaded separately. Sometimes the system will recognize the hardware but will be unable to load the modules due to some hardware or setup inconsistencies or version dependencies.

- **dmesg**. This is a command that you can run anytime and will display many of the messages that you see on bootup.
- **Mail**. TurboLinux will mail you a copy of the configuration and bootup messages for every reboot. This can be more extensive than the messages from `dmesg`. To get access to these messages type `mail`.
- **turbohw**. The `turbohw` command will probe your TurboLinux system and will give you a listing of hardware that it finds. It also allows you to generate a text file with detailed information on the hardware installed in your machine, including currently used resources (for example, IRQ, IO ports).

5.8 Server Services

Linux uses a concept of runlevels (0-6) to help manage the operation of the system. On boot, the system reads the file /etc/inittab to determine which runlevel it should enter. It then reads the subdirectories under /etc/rc.d that conform to that runlevel. The runlevel directories are:

- /etc/rc.d/rc0.d
- /etc/rc.d/rc1.d
- /etc/rc.d/rc2.d
- /etc/rc.d/rc3.d
- /etc/rc.d/rc4.d
- /etc/rc.d/rc5.d
- /etc/rc.d/rc6.d

For example, if the runlevel is set to 3, which is the level TurboLinux sets if you ask for a text-mode login during the install, the system reads the directory /etc/rc.d/rc3.d/ and starts or stops services based on the scripts in that directory.

The directory contains a number of symbolic links that point to scripts created to start, stop, and restart all the services provided by Linux. Looking at the directory, you will notice the files look similar. Below are a few examples from /etc/rc.d/rc3.d:

```
S10network
S11portmap
S14nfslock
S15nfsfs
```

You can see that they conform to the format [K or S][number less than 100][filename]. Each part may be explained as follows:

- The letter S denotes that this service should be started when entering the runlevel. The letter K indicates the services that will be killed when entering a runlevel from another runlevel.
- Services are started in order of the number here, with the lowest numbers being started first.
- the name of the script to run. The scripts reside in /etc/rc.d/init.d.

Runlevels are user configurable, but the conventional assignments in Linux (which TurboLinux follows) are:

- 0 -- Shut down the machine
- 1 -- Single user mode
- 2 -- Multiple user mode, but no networking
- 3 -- Full networking, text mode login
- 4 -- User configurable
- 5 -- Full networking, graphical login
- 6 -- Initiate a warm reboot

As we pointed out earlier, runlevels are user configurable, and TurboLinux provides the tool turboservice to edit the services run at each runlevel. When you start turboservice, it presents you with the following window:

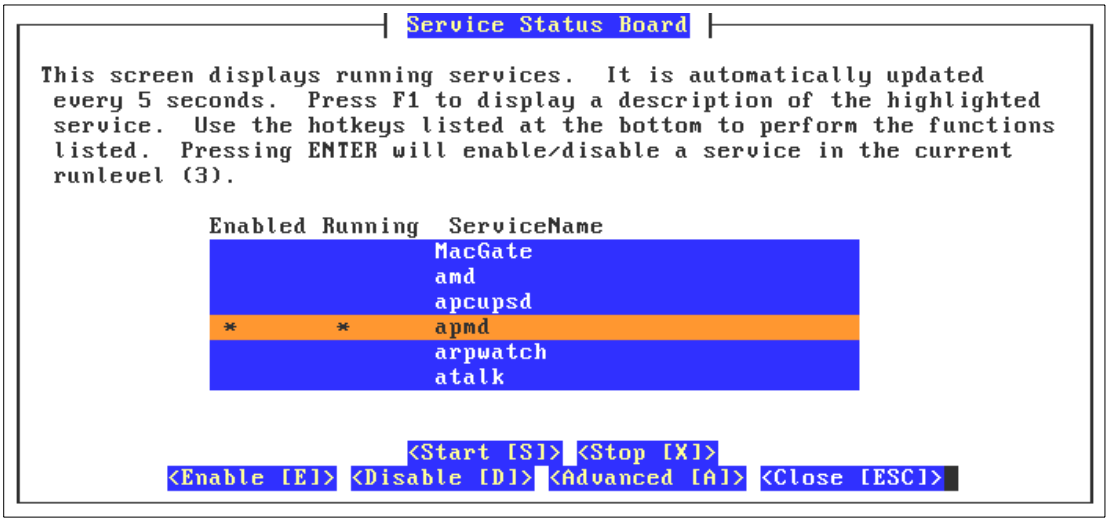


Figure 173. Service Status Board window

Notice that on this window, runlevels are not mentioned. That is because the main screen of turboservice runs in the current runlevel. In this case we are running at runlevel 3, so all the changes we make will be written to

/etc/rc.d/rc3.d/. Once turboservice is running, the columns are laid out in an easy-to-understand format:

- An * in the **Enabled** column means that TurboLinux will try to start this service when the runlevel is started.
- An * in the **Running** column means that the service is running at the moment.

The options at the bottom of the window are also simple: You can **Start** or **Stop** a service, as well as choose to **Enable** or **Disable** a service.

Selecting the **Advanced** option takes you the window shown in Figure 174. Here you can choose to enable services to start in runlevels 1-5.

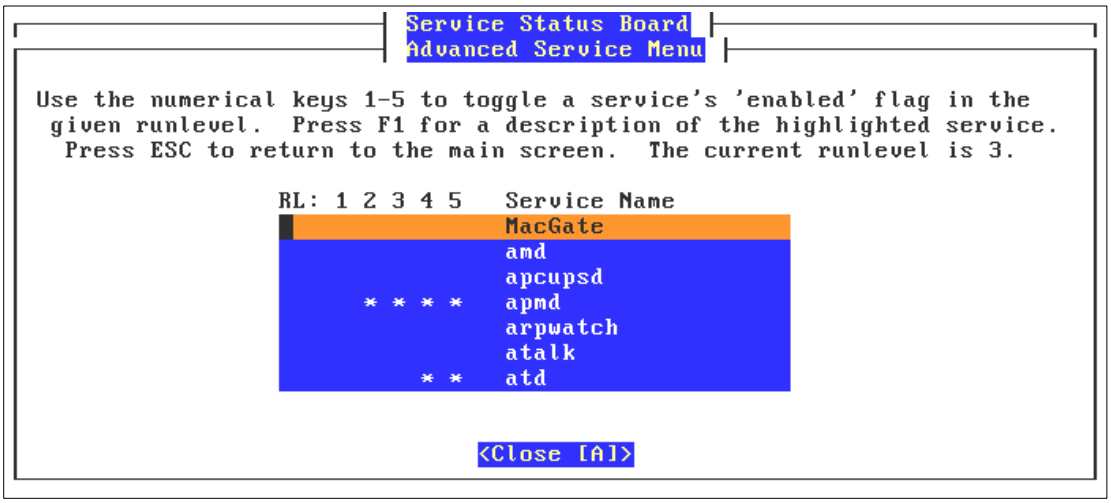


Figure 174. Advanced Service Menu window

Turboservice does not edit the services to stop. If you would like to do that, you must create symbolic links from /etc/rc.d/init.d/ to the runlevel you would like to edit. For example, if you wanted your Web server to stop if you entered runlevel 2, you would type the following command:

```
ln -s /etc/rc.d/initd/httpd /etc/rc.d/rc2.d/K15httpd
```

Of course, you could use a number other than 15. We use it here because that is the default for the HTTPD service.

5.9 Time zone and time server configuration

Setting the time zone on a server can be a non-trivial consideration in large environments. TurboLinux provides a single interface that can be used to configure time zone and time server properties.

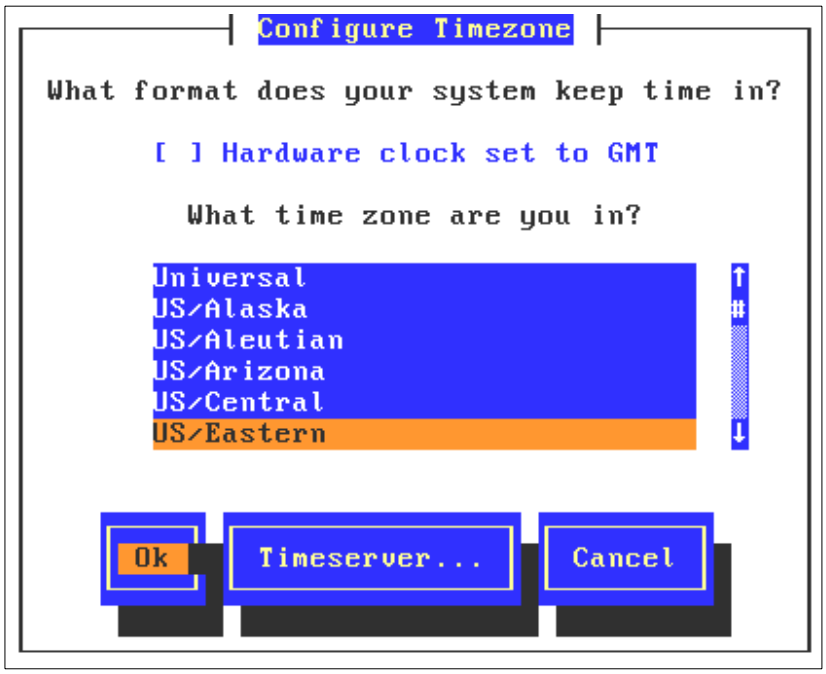


Figure 175. Configure Timezone window

By default, Linux uses the hardware clock in your server to set time. Setting the hardware clock to GMT is a good idea if clients will be logging into your server from other time zones, since the profile for each user can contain their time zone adjustment. If the clock on your server is set to local time, leave the option **Hardware clock set to GMT** unselected.

Choosing the correct time zone for this server is required whether or not the hardware clock is set to GMT.

On the bottom of the window you have an option to have the time for Linux set by a remote Timeserver instead of the local clock.

Selecting the **Timeserver** option generates Figure 176. You have options to connect to an NTP or RDATE based timeserver, and an option of resyncing the clock with varying frequencies.

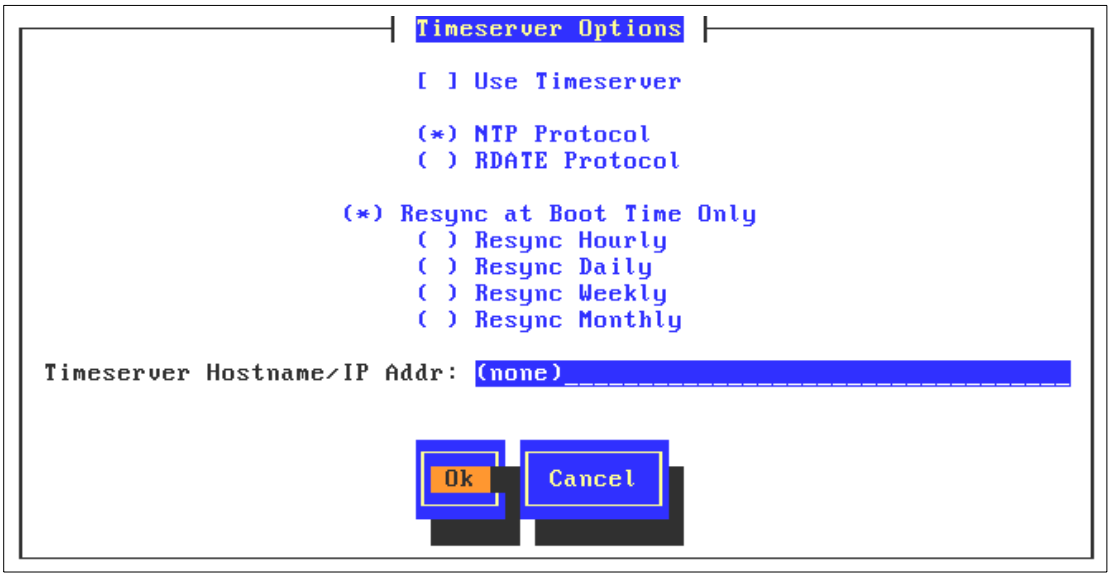


Figure 176. Timeserver Options window

5.10 Enabling remote services to your server

Linux provides two different ways to start server services such as FTP or a Web server. You can either start them separately in “stand-alone mode” through the runlevel structure (/etc/rc.d/rcX.d), or you can have them wait until a client machine requests the service. This second method is done through the program inetd, often called the “super server” because of its role. TurboLinux also comes with xinetd, a newer “super server” that offers more flexibility and features than inetd. However, inetd is the default in TurboLinux, so we will address it in this chapter.

By default, inetd is started in all runlevels that have networking support. Inetd monitors all TCPIP ports, and starts programs when a request comes to one of the well-known ports on any of the server’s interfaces. The well-known TCP/IP ports are defined in the flat text file /etc/services. As usual, inetd is configured in a plain-text file, this time the file /etc/inetd.conf. Figure 177 is the top part of the file. The rest of the file of organized in much the same way:

```
#inetd.conf This file describes the services that will be available
# through the INETD TCP/IP super server. To re-configure
# the running INETD process, edit this file, then send the
# INETD process a SIGHUP signal:'killall -HUP inetd'
#
# Version:/etc/inetd.conf6.0 Mar 12 2000
#
# Format:
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
#
# For security reasons, all services are turned off by default. Uncomment (or
# add lines) to have services started by inetd (see inetd.conf(8)for details).
#
# Don't forget to also edit /etc/hosts.allow for services which are started
# through tcp_wrappers (/usr/sbin/tcpd in the configuration lines below).
#
# Note: Some servers (typical examples: Web servers like Apache and MTAs like
#       Sendmail) run usually in stand alone mode, i.e. they are _not_ started
#       by the inetd. They are started at boot time (or manually) and keep
#       running.
##############################################################################
# ProFTP (standard TurboLinux ftp server)
# Warning: the authentication information for ftp goes as clear text over
# the net. This is especially dangerous if the same login/password combination
# can be used for any shell logins (telnet, ssh). Make sure remote ftp users
# have either /usr/bin/ftponly or /usr/bin/passwd as their login "shells".
# If you choose passwd, they can change their ftp password using telnet
# without having a real shell account on your system.
ftp    stream   tcpnowaitroot/usr/sbin/tcpdin.proftpd
##############################################################################
# WU ftpd (an alternative ftp server)
#ftp  stream   tcpnowaitroot/usr/sbin/tcpdin.ftpd -l -a
##############################################################################
# Telnet
# Warning: telnet is inherently insecure as a protocol. All network traffic,
# including authentication information (login and password) are transmitted
# as clear text. Look for secure alternatives (e.g. ssh).
# The -h option prevents your telnetd from giving away information which
# may be useful for potential system crackers. See telnetd(8) for details.
#telnet stream tcp nowaitroot/usr/sbin/tcpdin.telnetd -h
##############################################################################
# POP3 mail server
#pop-3   stream  tcp     nowait  root    /usr/sbin/tcpdipop3d
##############################################################################
```

Figure 177. inetd.conf file

As you can see from the selection of /etc/inetd.conf, the comments explain what services can be run, and give some warnings as well. In the example above we have enabled the ProFTP server by removing the # at the beginning of the line shown in bold.

The networking subsystem maintains two more files for security purposes that will have to be edited in order for remote users to access an FTP server

on this system. The files are /etc/hosts.allow and /etc/hosts.deny. We will discuss them now.

The default /etc/hosts.allow is listed below:

```
hosts.allow   This file describes the names of the hosts which are
#               allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
#
# See man hosts_access(5) for more information

ALL : 127.0.0.1
```

Figure 178. hosts.allow file

In order to allow other computers on the network to access this server, you will have to add the line

```
ALL : ALL
```

This will enable your remote access.

You also need to edit the /etc/hosts.deny file. In Figure 179, you will notice that access is denied to all systems, including the localhost. This will also prevent access to any systems, even though it is specified in the /etc/hosts.allow file.

```
#
# hosts.deny    This file describes the names of the hosts which are
#               *not* allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
#
# See man hosts_access(5) for more information.

ALL: ALL
```

Figure 179. Hosts.deny file

In order to allow access from all remote hosts you need to change the last line in Figure 179 to the following:

```
# ALL: ALL
```

Adding a # at the front of the line disables the exclusion, thus allowing the hosts.allow file to give access to your system. The next time inetd is started, your FTP server will be available to hosts on your network. To restart inetd immediately, type the command

```
killall -HUP inetd
```

5.11 File system permissions

Linux has inherent security features, the most noticeable being file system permissions. Setting permissions on files allows the system administrator to restrict access to parts of the file system.

File permissions can be set on files and directories. The easiest way to see an example of this is looking in the /home directory:

```
mail:/home # ls -l
total 1
drwxr-xr-x  19 root     root          396 Nov 15 21:06 .
drwxr-xr-x  22 root     root          467 Nov 13 16:28 ..
drwx------   6 davej    users         912 Nov 15 21:05 davej
drwx------   6 george   users         912 Nov 15 21:03 george
drwx------   6 ivo      users         912 Nov 15 21:02 ivo
drwx------   6 jakob    users         912 Nov 15 21:03 jakob
drwx------   6 jasmin   users         912 Nov 15 21:04 jasmin
drwx------   6 jens     users         912 Nov 15 21:04 jens
drwx------   6 jhaskins users         912 Nov 15 21:02 jhaskins
drwx------   6 justin   users         912 Nov 15 21:06 justin
drwx------   6 lenz     users         912 Nov 15 21:03 lenz
drwx------   6 linux    users         912 Nov 15 21:03 linux
drwx------   6 malcom   users         912 Nov 15 21:04 malcom
drwx------   6 rachael  users         912 Nov 15 21:03 rachael
drwx------   6 rafiu    users         912 Nov 15 21:04 rafiu
drwx------   6 ruediger users         912 Nov 15 21:04 ruediger
drwx------   6 rufus    users         912 Nov 15 21:02 rufus
drwx------   6 ted      users         912 Nov 15 21:03 ted
drwx------   6 uzi      users         912 Nov 15 21:04 uzi
mail:/home #
```

Figure 180. Viewing file permissions

Taking the user “linux” as an example:

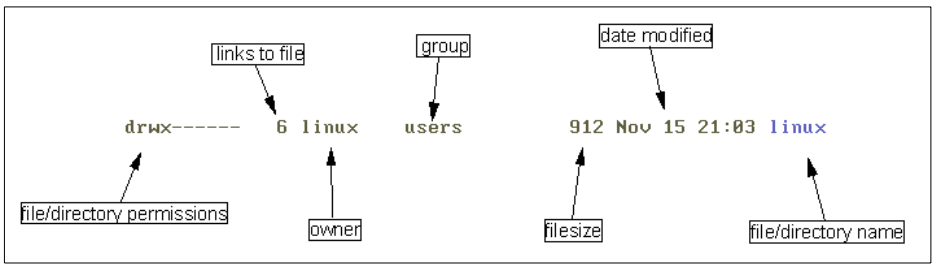


*Figure 181. Explanation of **ls** output*

What we are most interested in is the file/directory permissions. This signifies a lot of information in a short amount of space:

d - The first character in the permissions signifies that this is a **d**irectory. Other files are represented by:

- - a normal file.

l - a symbolic link to another file.

c - refers to files in the /dev directory. This signifies the file represents a character device.

b - refers to files in the /dev directory. This signifies the file represents a block device.

rwx - In this case it allows only the owner of the file (in this case “linux”) to read, write and execute this file.

Type	Owner	Group	World
d	rwx	---	---

The owner of the file is the user that created the file. The group part is the group that owns the file (for example, the group **users**). The world part means everyone else; setting a permission in the world part sets the permission for every user, irrelevant of their group membership and so on.

Here is another example:

-rwxr-xr--

This means that this is a normal file, the owner can read, write and execute the file, the group can read and execute the file, and everyone else can read the file, but not modify or execute it.

If you set a directory as:

drwxrw-rw-

you are saying that only the directory owner is allowed to execute something “inside” the directory. So if another user tries to change directory into this directory, they will get a “permission denied” error message. This is exactly what happens with regards to users’ home directories.

To change the permissions on a file, you use the **chmod** command. Only *root* can modify files that do not belong to them. You must own the file to be able to change its permissions.

The easiest way to change permissions is to use symbolic representations of what you want permissions to be.

Note

The other way to represent file permissions is to use octals. For more information about this and the `chmod` command see the `chmod` man page.

```
chmod g+rw myfile
```

The command above is one of the simplest ways of changing a permission. You are saying that you want the file `myfile` to allow all members of the group to be able to read and write to it.

If you used a **-** (minus sign) instead of a plus, you would be taking away those permissions. This would mean that members of the group would not be allowed to read or write to the file.

You can mix adding and removing permissions in the same command:

```
chmod u+x-rw myfile
```

This will allow executing the file, but will not allow reading or writing the file for the file owner.

Here is a summary of the symbolic representations available in chmod:

r - read

w - write

x - execute

- - take away the permissions

+ - add the permissions

s - set the SUID bit. This says that if the file is executable, it will be run as the owner of the file, not as the user that is running the file.

Chapter 6. Backup and recovery

One of the items system administrators should maintain are well-established routines for backup and recovery.

Your data is very valuable. If it is lost, it costs you time and money to recreate them. If you are unable to recreate the information, it could devastate your business or operation.

Some of the reasons you can lose your data are hardware failures, software malfunctions, human failures, and natural disaster. Modern hardware is quite reliable, but still may fail. The most critical parts of hardware for storing data are hard disks. The different levels of RAID implementations minimize the consequences of hard disk failures. But even a RAID configuraton may fail for one reason or the other. Software is unreliable by nature. Humans can make errors or can be malicious and try to destroy data.

Therefore, back up your data.

If you back up your data, be sure that the restoration and recovery of data from the backup media works reliably.

The term *recovery* implies the restoring of files from backup tape(s) in a production environment and the recovery of a whole system after a possible disk crash. Backup and recovery are mainly planning and organizational tasks. The managing and protecting of your data utilizing a Linux operating system can easily be accomplished with commercially available products (for example, BRU, Arkeia, BackupEDGE, etc.).

In a Linux environment, backup devices are named /dev/stx for the x-th rewinding and /dev/nstx for the x-th nonrewinding tape SCSI-device. ATAPI tape devices or “floppy” tape drives that some backup packages support may use a different naming scheme.

For more in-depth information about backup strategy, media and hardware, consult the IBM Redbook, *Netfinity Tape Solutions*, SG24-5218. This redbook can be downloaded from the following Web site:
`http://www.redbooks.ibm.com/`.

You can also find valuable information in *The Linux System Administrator’s Guide* by Lars Wirzenius and Joanna Oja. This book can be obtained in PDF format from the following Web site: `http://www.linuxdoc.org/`, then search on *Backup Media*.

© Copyright IBM Corp. 2001

Your first step in putting together a viable backup solution is to choose the backup media. It should be removable and stored in a safe place. It cannot be one of the disk drives in your system. Your selection of media should be either floppy, floppy tape, tape, ZIP media, or magneto-optical disk. Using floppies as backup media can be unsuitable if a large amount of data should be backed up and/or unattended operation is an important issue. Mostly, SCSI or ATAPI tape are a suitable choice. The cost and availability may help you decide. If SCSI tape is your preferred choice, you have to choose between QIC, DAT, EXABYTE or DLT tapes of different capacities. The amount of data to be backed up and the cost of the backup device(s) and media may determine your decision. Some of the backup packages support tape libraries.

Choosing the right backup media may also depend on the backup tool you want to use and whether it supports your media.

Every IBM @server xSeries and Netfinity system has a built-in SCSI controller. We recommend you choose a SCSI device for your backup. You can choose between different technologies (QIC, DAT, EXABYTE, or DLT) depending on the amount of data to be stored and the speed required.

6.1 Backup Hardware

The tape products listed in Table 8 are currently available for IBM @server xSeries and Netfinity servers and support at least one backup/restore package by Linux:

Table 8. Linux backup tools, supported by Netfinity tape devices

Tape device	Arkeia	BackupEDGE	BRU
IBM 35/70 GB DLT tape drive (SCSI-2	x	x	x
IBM 20/40 GB DLT tape drive (SCSI-2)	x	x	x
IBM 20/40 GB 8 mm tape drive (SCSI)	x	x	x
IBM 10/20 GB NS tape drive (SCSI-2)	x	x	x
IBM 100/200 GB Internal LTO Tape Drive (SCSI-2)	x	x	x

Tape device	Arkeia	BackupEDGE	BRU
IBM 4/8 GB TR4 tape drive (SCSI-2 or EIDE)	x (only SCSI)	x	x
IBM 3447 DLT tape library (SCSI-2)	x	?	
IBM 3449 8 mm tape library (SCSI-2)		?	
IBM 3575 Magstar MP tape library (SCSI)	x	?	

For more information about the features of these tape devices, please consult *Netfinity Tape Solutions*, SG24-5218, or the following Web sites:

`http://www.ibm.com/storage`
`http://www.redbooks.ibm.com/`

Notes

Since Linux supports all SCSI tape devices, Linux should not depend on the technical characteristics of the tape drive used (for instance AIT, DAT, DLT, Exabyte, LTO, or QIC).

If you use tape libraries or autochangers, please enable the kernel option to probe all LUNs on each SCSI device. The tape drive and the changer may use the same SCSI-ID, but different LUNs.

We recommend that you do not connect tape devices to the IBM ServeRAID adapter. Use a separate SCSI controller for the tape devices.

6.2 Backup strategy

The next issue to resolve is to determine what data to back up and when. Your first backup must be a full backup of your system. This can take a long time and may require more than one backup medium depending of the amount of data to be backed up. These dependencies influence when you can run a full backup. After this first full backup, you can run incremental backups, which means backing up only those files that have changed after the last full or incremental backup. It is good practice to use different backup media for full and incremental backups. But take into account that restoring the data after a system crash requires the last full backup and all following

incremental backups in their correct order. Since this can be very time consuming, you should plan a scheme for periodic backups very carefully. A suitable scheme may be one full backup per week during off hours and incremental backups on the other days. Whether you need more than one incremental backup per day depends on the amount of data that has changed and how critical your data may be.

For your full backup media use the scheme Grandfather - Father - Son. This means, that you normally have three generations of backed up data. During the new full backup, when the grandfather becomes the new son, you have at least two generations of data to use, if the system crashes during this operation. If the creation of a new backup finishes successfully, the media for incremental backup can be reused again.

6.3 Backup tools

To back up your data, you can use one of the archiving tools that are already available on your system. Tar, cpio, dump are only some of these tools. But take into account that you have a lot to do to use one of these tools comfortably.

You should consider using one of the third-party products we mentioned earlier (BRU, Arkeia, or BackupEDGE/RecoverEDGE) for your backup tool. They come with a command line interface, so you have full control over the tools' functionality, and you also have the use of a graphical interface. These products should include a scheduler to make it easier for you to set up the periodic scheduling scheme most comfortable for you.

Information on the commercially available backup solutions can be found at the following Web sites:

Arkeia:	`http://www.arkeia.com`
BRU/CRU:	`http://www.estinc.com`
BackupEDGE/RecoverEDGE:	`http://www.microlite.com`

Detailed information on the installation and configuration of these products on IBM @server xSeries and Netfinity servers can be found in Chapter 7, "Backup applications install and setup" on page 181:

6.3.1 BRU and CRU

BRU (Backup and Recovery Utility) is the backup and restore solution from Enhanced Software Technologies (Web site: `www.estinc.com`). It is a backup and restore utility with significant enhancements over other common utilities

such as tar, cpio, volcopy and dump. BRU is designed to work with most backup devices, including cartridge, 4mm DAT, 8mm (Exabyte) and 9-track tape drives.

BRU includes incremental backups, full backups, multivolume archives, distribution and updates, error detection and recovery, random access capabilities, file comparisons, and file overwrite protection.

As part of the package, BRU also contains a graphical user interface (GUI) named XBRU. Used from the command line, BRU is very similar to Tar. The dialog windows of XBRU are very intuitive and easy to use. To set up a scheme for scheduled backups, it is easiest to use the BRU for X11 Scheduler component of XBRU.

CRU (Crash Recovery Utility) is the recovery solution from Enhanced Software Technologies. It allows you to recover your system after a disaster crash.

To use CRU, you must create two floppy disks (a boot disk and a root disk) and/or a bootable CD-ROM, which are used to start the system recovery after a disaster crash. Follow the instructions in the CRU documentation to create the boot media. After every change in the system layout, mainly the layout of the hard disks, you have to repeat the creation of the CRU boot and root disks.

CRU requires that you create a special full backup tape using CRU. This backup feature of CRU can replace the corresponding BRU feature to create full backups.

6.3.2 BackupEDGE and RecoverEDGE

BackupEDGE is the backup and restore solution from MicroLite (Web site: `www.microlite.com`). It supports SCSI and ATAPI tapes as well as some tape libraries. For more information, check MicroLite's Web page and search on *Device Compatibility* to obtain a list of the supported tape drives and autochangers.

RecoverEdge is the recovery solution from MicroLite. It allows you to recover your system after irreparable damage has been done to the system disk.

You have to create some floppy disks (boot disk, root disk, and maybe a second root disk) and/or a bootable CD-R, which are used to boot from to begin a disaster recovery of your system. It is necessary to create these disks after every change in your system configuration, mainly after every change in

the layout of the system disks. Following a well-planned backup scheme is also a prerequisite.

To recover after a disaster crash, you need the last full backup media and all subsequent incremental backup media created with BackupEDGE.

6.3.3 Arkeia

Arkeia is a backup and restore solution that allows centralized network backup in a client/server architecture. With Arkeia, you can also back up UNIX, Windows, Windows NT or Novell clients.

With Arkeia you can safely archive every file, directory, device node and special file on your file systems, unlike the standard UNIX `tar` command, which ignores many important files. Arkeia also verifies the data written to tape to ensure that the tape is an accurate reflection of your data. The following are features provided by Arkeia backup software:

- Data compression - automatic data compression is supported.
- GUI and CLI interface.
- The backup server may be your local system or a remote system.
- High performance - advanced double buffering and variable block factors.
- Virtual file support - you can back up virtual (sparse) files.
- Multi-volume / multi-device archives - automatic spanning across multiple volumes or devices.
- Wildcard support - when selecting files you can use a wildcard.
- Raw device backups - you can archive an entire raw device/partition to tape.
- Master / incremental backups.
- Unattended operation - you can configure schemes to periodically perform full backups and/or incremental backups.

Arkeia is designed to operate on Linux kernels 2.x and there are versions available for several types of libraries (libc5 and libc6) and distributions. Arkeia supports only devices connected to SCSI-controllers and also tape libraries.

You can find Arkeia's Web site at `http://www.arkeia.com`.

Chapter 7. Backup applications install and setup

It may seem obvious that backing up and restoring data quickly is critical, but many administrators leave this task at the end of the “to do” list until it is too late. With the ease of use of the commercially available packages BRU (Enhanced Software Technologies), BackupEDGE/RecoverEDGE (MicroLite) or Arkeia (Knox Software), there is no need to wait.

Note

We recommend that you do not connect tape devices to the IBM ServeRAID adapter. Use a separate SCSI controller for the tape devices.

7.1 BRU

BRU is a backup and restore utility with significant enhancements over other common utilities such as tar, cpio, volcopy and dump. BRU is designed to work with most backup devices, including cartridge, 4mm DAT, 8mm (Exabyte) and 9-track tape drives.

BRU includes incremental backups, full backups, multivolume archives, distribution and updates, error detection and recovery, random access capabilities, file comparisons, file overwrite protection, and increased speed over previous versions.

7.1.1 Installing BRU

Before you begin, you need to know the following:

1. The device name of your tape drive. Typically under Linux, this will be /dev/st0 for the rewinding and /dev/nst0 for the non-rewinding drive.
2. The size of your backup medium in megabytes.

   To install BRU from the floppy drive with the `tar` command, type:

```
cd /tmp
tar xvf /dev/fd0
./install
```

Follow the prompts regarding readme files and licenses, enter your *license data* and your *BRU serial number* when asked to do so until you come to the following window:

© Copyright IBM Corp. 2001

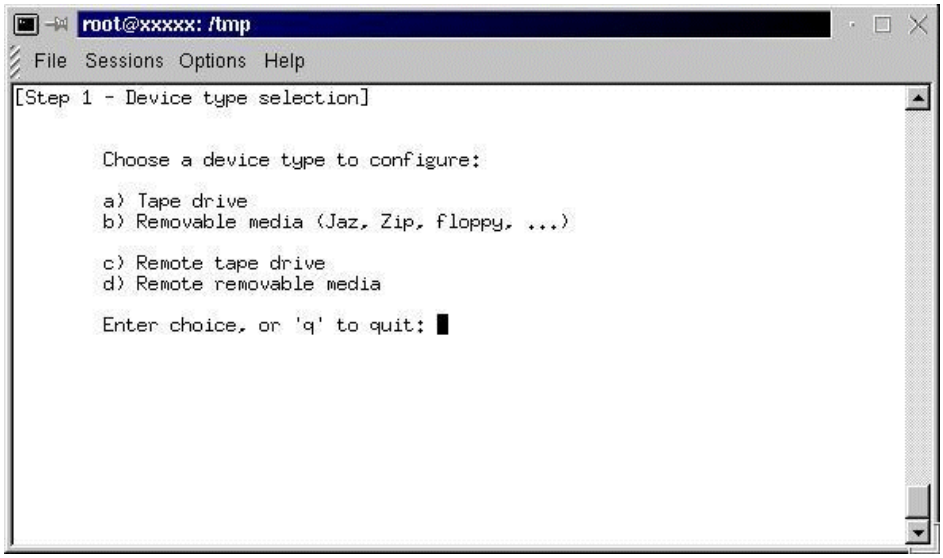


Figure 182. Selecting your backup devices

Enter the letter for your backup device and answer the following questions appropriate for your device.

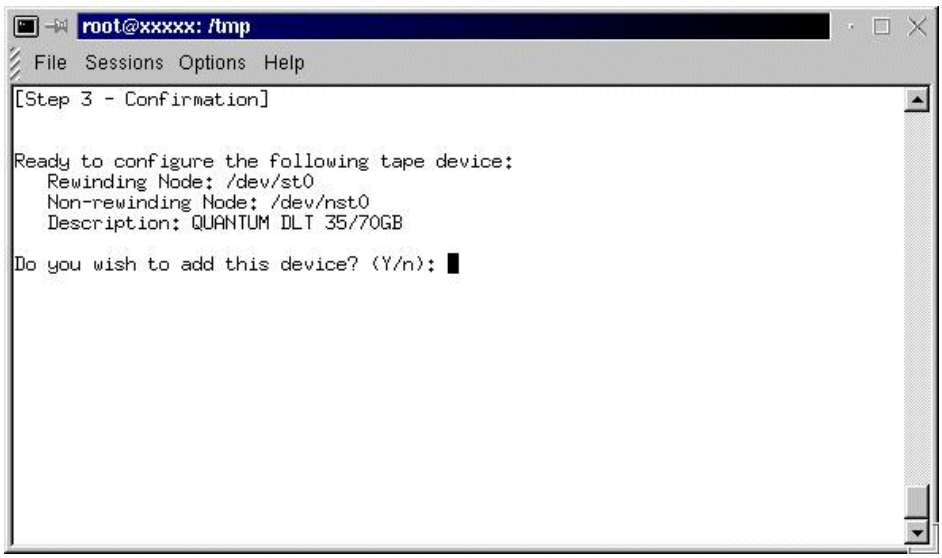


Figure 183. You have entered your backup devices

If you have entered the information for all your backup devices, you will be asked if you would like to install the X11 interface. Select **Y**.

The installation program needs to create an xbru directory. You can select a path or accept the default /usr/local/.

The installation program will install executables in a user-specified directory. The default is /usr/local/bin.

Note

The key configuration file is /etc/brutab. Consult the *BRU User's Guide* for advanced information. Do not edit unless you know what you are doing.

BRU is now installed.

7.1.2 Basic commands

The basic command structure for BRU is:

```
# bru modes [control options] [selection options] [files]
```

Where `bru` is the command or program followed by the mode specifying backup, restore, or various queries. `Control options` specify devices and buffer size. `Selection options` control which files or directories to work with. `Files` is the specified target of the `bru` command.

7.1.3 Basic backup

To back up a single file /home/ayne/.profile:

```
# bru -c -vvvv -G /home/ayne/.profile
```

To back up the complete directory /home/ayne:

```
# bru -c -vvvv -G /home/ayne
```

To back up the entire system:

```
# bru -c -vvvv -G /
```

7.1.4 Basic restore

To restore a single file /home/ayne/.profile:

```
# bru -x -vvvv -ua -w /home/ayne/.profile
```

To restore the complete directory /home/ayne:

```
# bru -x -vvvv -ua -w /home/ayne
```

To restore the entire system:

```
# bru -x -vvvv -ua -w /
```

7.1.5 Basic verification and listing commands

The -i mode can be used in conjunction with a backup command or by itself. The -i mode reads each block of data and verifies the checksum of the block. If used with the verbosity options (-vvvv), BRU will give a complete listing of the contents of an archive.

The `-G` mode displays the archive header block, which contains detailed information on the archive including the command used to create the archive. See the *BRU User's Guide* for more information.

The `-gg` mode displays the contents of the on-tape directory. This mode can only be used if the archive was created with the `-G` option.

7.1.6 X Interface

To use BRU's X interface, you will need to be in an X-Windows environment. Type:

```
xbru
```

Figure 184. XBRU window

You will see a window similar to Figure 184.

From this interface you can:

- Create and restore backups.
- Create save, and load backup definitions.
- Schedule backups.
- List and verify the contents of archives.
- View the BRU log.

7.1.7 The big buttons in BRU

The three main buttons (Full, Level 1, and Level 2) are shortcuts to various levels of backing up your system, directories, or individual files.

- Select **Full** to back up all the files in the user's home directory, or, if the user is root, the entire system.

- Select **Level 1** to execute a backup for the same files as listed above, on the condition that files have been modified since the previous full backup. If no previous full backup has been done, this will be considered a full backup.
- Select **Level 2** to execute a backup for the same files as listed above, on the condition that files have been modified since the previous level 1 backup. If no previous level 1 backup has been done, this will be considered a level 1 backup.

7.1.8 Creating archives

Creating archives with BRU's X interface is simple. Click the **Backup** button to bring up the Backup File Selection interface (Figure 185).

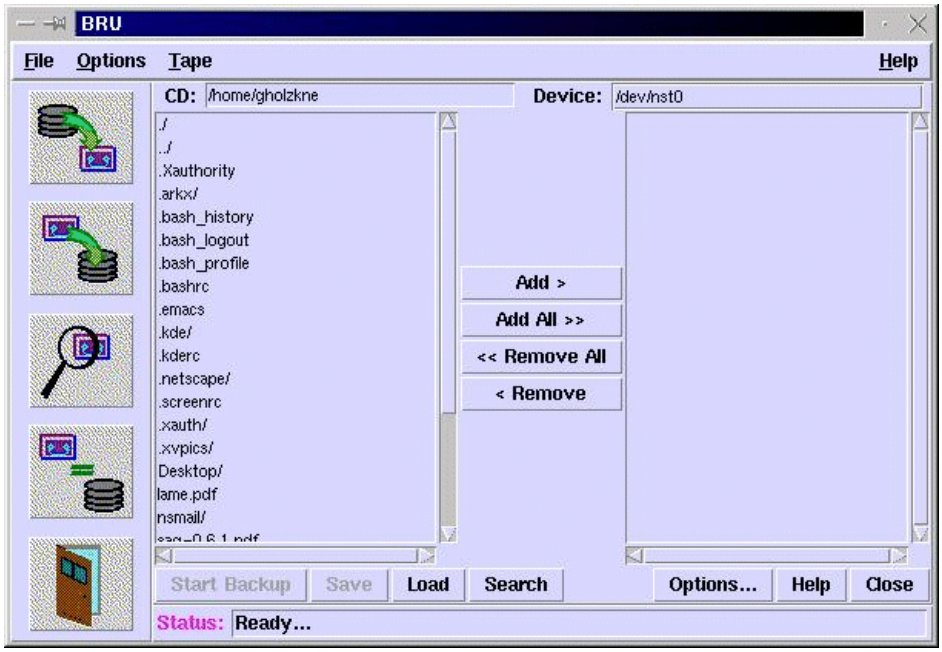


Figure 185. Creating an archive

The box on the left displays the contents of the current directory (CD:). You can change the current directory by editing the CD entry. Then press Enter.

You can add or remove files and directories from the backup list by selecting them and clicking the appropriate button.

BRU also provides a search function. Click the **Search** button to bring up a dialog box prompting you for a search string. This string can contain typical wildcards.

Backup Definitions are a way to define a set of commonly used backup options or preferences for use at a future time. You can create definitions for use with the backup scheduler or simply use the default selections.

After you have selected the files and directories that you wish to back up, you can click the **Options** button. In this dialog (Figure 186) you can set your preferences regarding different options. After you have made your decisions, click the **Close** button to return to the previous dialog. To start the backup click the **Start Backup** button.

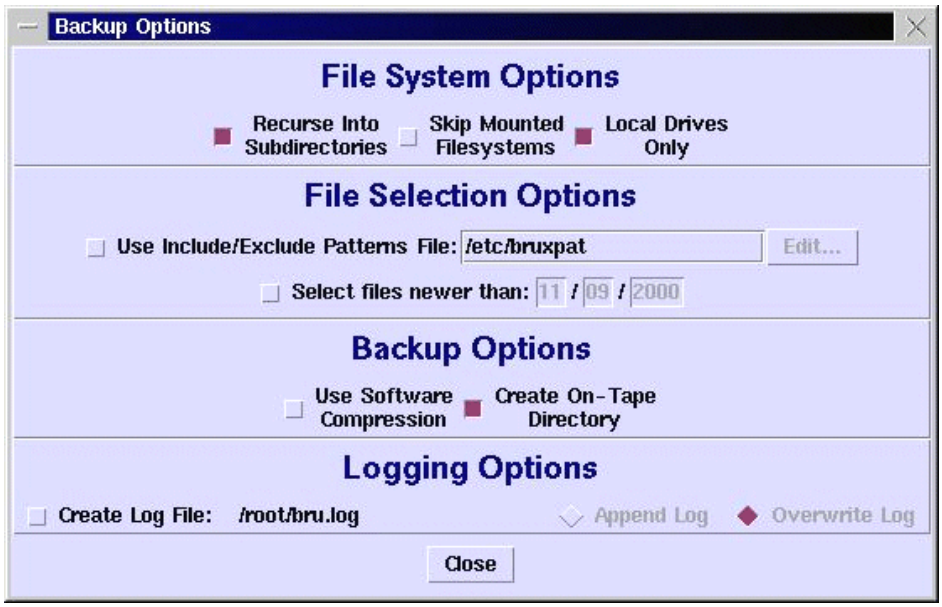


Figure 186. Dialog for backup options

Enter in the next dialog, click **Enter Archive Label** and enter text to identify your new archive. Click **Create Backup** to proceed.

The backup will inform you of how many directories/files and which amount of data will be backed up. During backup, you see a window, informing you about the progress and the actual action. When the backup process has finished, click **Done** to return to XBRU's main dialog.

7.1.9 Scheduling

To access the scheduling feature, go to **File>Scheduler** on the menu.

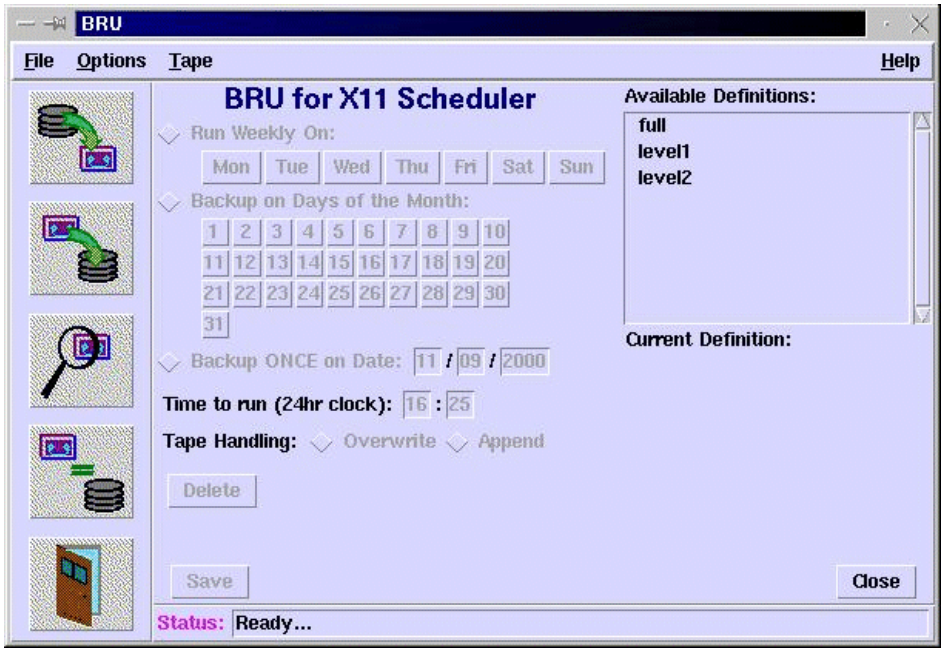


Figure 187. Scheduler

BRU provides a scheduling utility to automate the backup process for the busy administrator. There are three predefined definitions: Full, Level 1, and Level 2. These are the same definitions used in 7.1.7, “The big buttons in BRU” on page 185. You can create your own definitions in the Creating Archives interface.

From the BRU for X11 Scheduler interface, you can set scheduled backups based on weekly, monthly, or single dates. The scheduler is very flexible. In order to take advantage of the scheduling options, you must save your desired schedule configuration and verify that the scheduler is being run from cron. To verify or add the cron entry, log in as root and type:

```
crontab -e
```

Insert the following line:

```
0/5 * * * * /usr/local/bin/bruschedule
```

If you chose a different path for the binaries during installation, change the entry accordingly.

Save the crontab entry. You can now schedule backups.

7.1.10 Restoring files

Restoring files with BRU's X interface is simple. BRU will retrieve the contents of the archive when you click the **Restore** button. After scanning the archive, the Restore File Selection interface (similar to Figure 185) will appear.

> **Note**
>
> If the on-tape directory is not in the archive, then BRU must scan the entire archive to get a listing. This can be very time consuming. When creating an archive, use the -G option to create the on-tape directory or chose **Create On-Tape Directory** in XBRU's O**ptions** dialog from the backup dialog.

The box on the left displays the contents of the current directory that is stored on the tape. You can change the current directory by editing the **CD:** entry and pressing Enter.

You can add or remove files and directories from the backup list by selecting them and selecting the appropriate button.

When you have selected all of the files and directories that you wish to restore, click the **Restore** button. A progress window will show each file as it is restored.

7.1.11 Listing and verifying archives

For listing the contents of an archive, BRU gives you three options:

1. Header - This option shows the archive header record, which lists the label, creation date, version, and serial number. For more information on the header, consult the *BRU User's Guide*.
2. Filenames only - This option displays the on-tape directory. If the archive was created without using the -G option, BRU will scan the entire archive to create a list of files. You will be prompted before this occurs, as this can be a lengthy process.
3. Full details - This option scans the entire archive for details such as file names, permissions, owners, size, modification times, etc. This process can be time consuming.

For verifying archives, BRU gives you two options:

1. Checksum Verification - When archives are written, a checksum is calculated for each block of data. The checksum is stored in the header of each block. Checksum verification will read each block, recalculate the checksum, and compare the checksum to the value in the header. Each file will be listed as it is verified, along with any errors found. If no errors are found, you know you have an accurate backup.
2. Compare Verification - BRU compares the files in the archive to the files on the hard drive. Any differences, such as modification times, size, or files in the archive that are nonexistent on the hard drive are noted. An *end of differences* notice will be posted when the verification is complete.

7.1.12 Summary

For information on advanced features consult your *BRU User's Guide* or the BRU Web site at:

```
http://www.estinc.com/
```

7.2 Microlite BackupEDGE

BackupEDGE is a complete backup solution for the Linux platform. It is easy to use and still very robust. With BackupEDGE you can safely archive every file, directory, device node and special file on your file systems. Unlike the standard UNIX tar command, which ignores many important files, BackupEDGE also verifies every byte of data written to the tape to ensure the tape is an accurate reflection of your data. Below are the features provided by BackupEDGE backup software:

- Data compression - automatic data compression is supported.
- Menu interface - almost all functions can be accessed through an intuitive menu system.
- Remote tape drive support - you can back up computers across the network.
- High performance - advanced double buffering and variable block factors.
- Virtual file support - you can back up virtual (sparse) files.
- Multi-volume / Multi-device archives - automatic spanning across multiple volumes or devices.
- Wildcard support - when selecting files you can use a wildcard.
- Raw device backups - you can archive an entire raw device/partition to tape.
- Master / incremental backups

- Unattended operation - you can perform a master backup or back up only the changed files.

BackupEDGE is designed to operate on Linux kernels 2.x and there are available versions for several types of libraries.

In the following sections we describe how to install, configure and use the Microlite BackupEDGE backup software.

Note

We recommend that you do not connect tape devices to the IBM ServeRAID adapter. Use a separate SCSI controller for the tape devices.

7.2.1 Installing Microlite BackupEDGE

Before you install BackupEDGE you must identify the device entry for your backup device. Usually tape devices under Linux are assigned in device nodes `/dev/st0, /dev/st1...` A no-rewind device is created for each tape device, which is `/dev/nst0, /dev/nst1...` In our example, we used `/dev/st0` as tape device and `/dev/nst1` as the no-rewind device.

In our example, we used diskette as the installation medium. To install the product, follow these steps:

1. Log in as root.
2. Change the directory to root "/".
3. Insert the diskette with the product in the floppy drive and execute the command:

   ```
   tar xvf /dev/fd0
   ```

   Where `/dev/fd0` is your floppy device.
4. Execute the following command to finish the installation:

   ```
   /tmp/init.edge
   ```

   You will see a window similar to Figure 188.

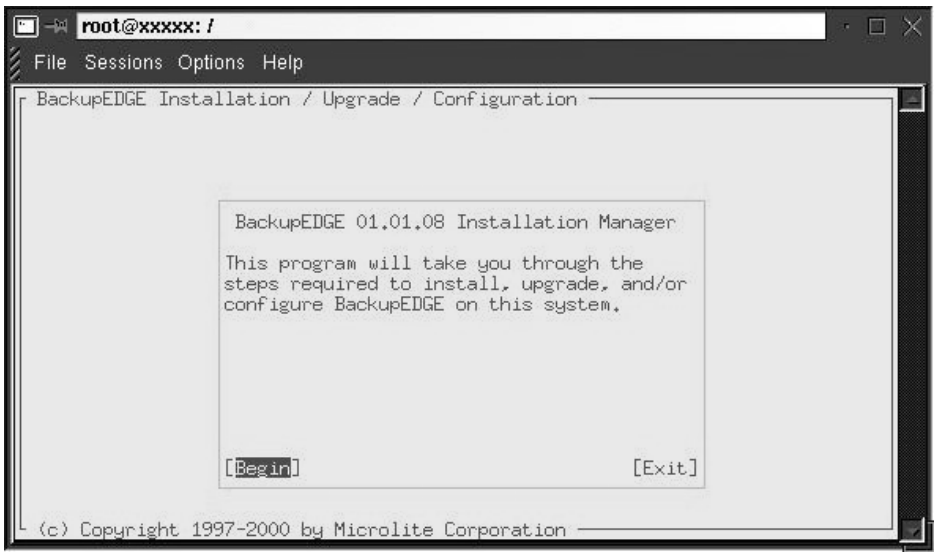


Figure 188. Start of installation dialog

The installation program guides you through the installation process. The windows are intuitive. During the installation process, you can also configure your backup device(s) and your scheduling schema for unattended operation. If information is needed during this process, you are asked to enter the appropriate data.

Now you are ready to use the product.

The actions *Resource Manager* and *Defining Devices* can be started by entering on the command line:

`/usr/lib/edge/bin/edge.resmgr` (Resource Manager) or

`/usr/bin/edge.config` (Defining Devices)

You can also perform these actions, if you click **Admin** on BackupEDGE's main window.

7.2.2 Initializing the tape

Before you start making backups you should initialize the tape. To do this, you follow these steps:

1. Start the edgemenu program by executing command:

   `edgemenu`

   You will see a window similar to Figure 189.

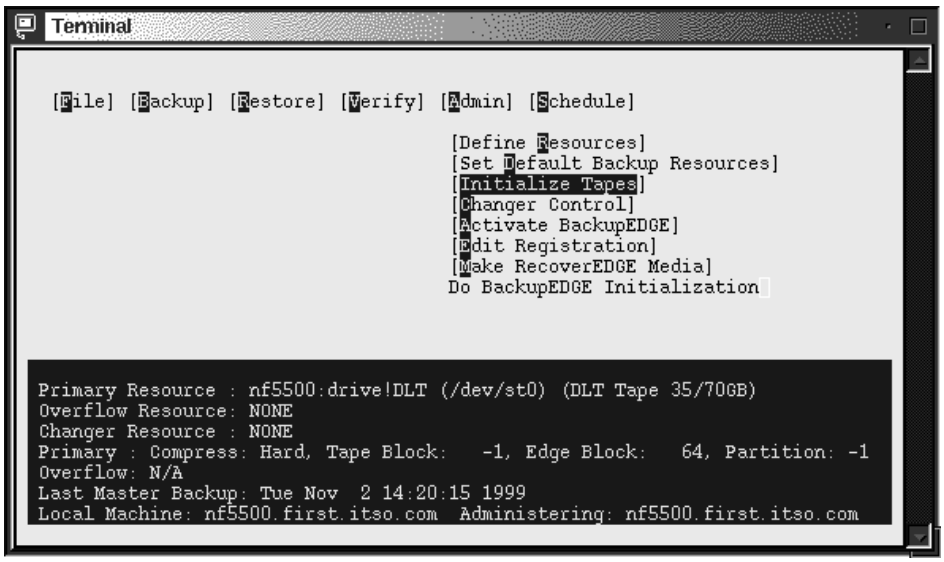


Figure 189. BackupEdge main menu

2. In the Admin menu select **Initialize Tapes.** You will see a window similar to Figure 190.

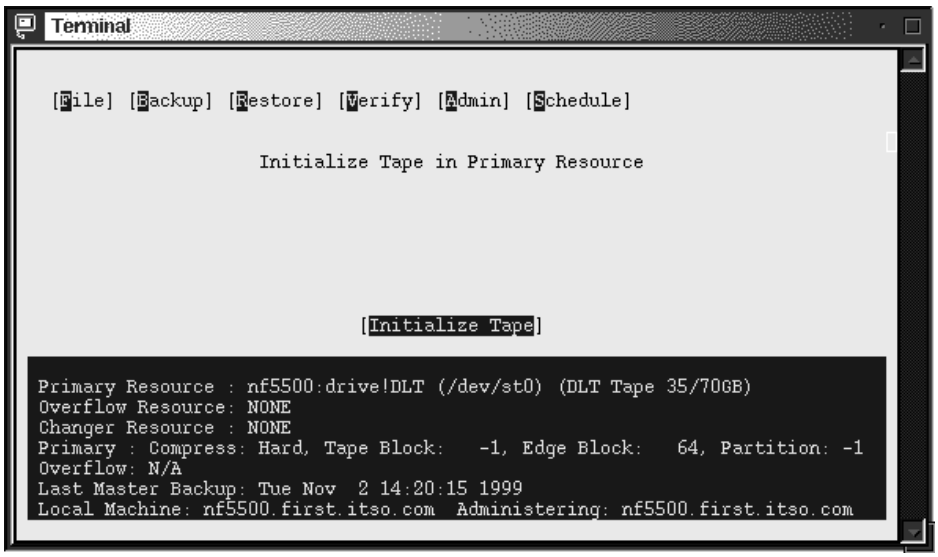


Figure 190. Initializing the tape

3. Select **Initialize Tape** and press Enter**.** The tape will be initialized. You will get a message that the tape is successfully initialized. Press Enter to continue.

You can check the tape properties by selecting **Show Tape Label** in the Verify menu. You will see a window similar to Figure 191.

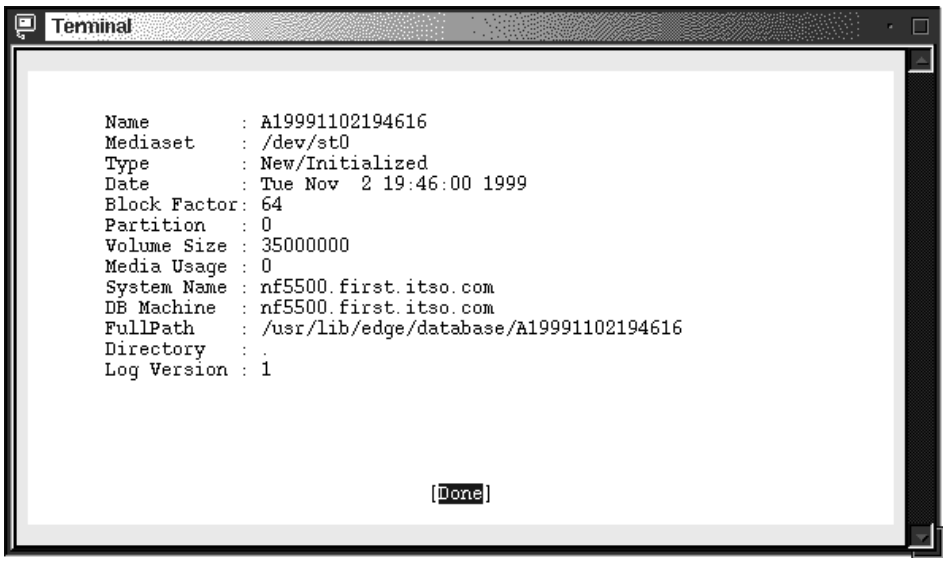


Figure 191. Tape information

7.2.3 Your first backup

In this section we will show how to make backups of desired files or directories. You can perform backups in the edgemenu utility. Follow these steps to make a sample backup:

1. Start the edgemenu program by executing the following command:

   ```
   /usr/bin/edgemenu
   ```

   You will see a window similar to Figure 192.

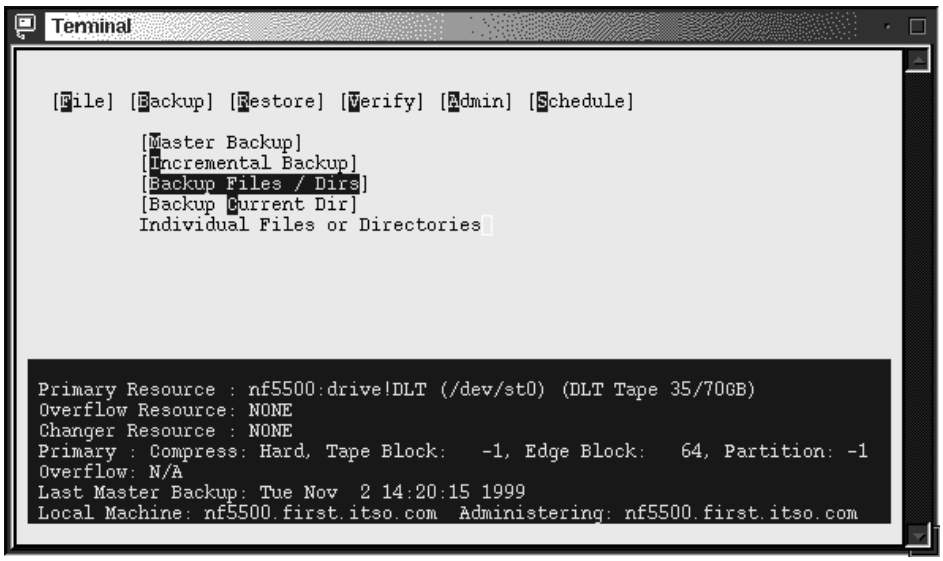


Figure 192. Starting the backup

2. In the Backup menu select **Backup Files / Dirs,** and you will see a window similar to Figure 193.

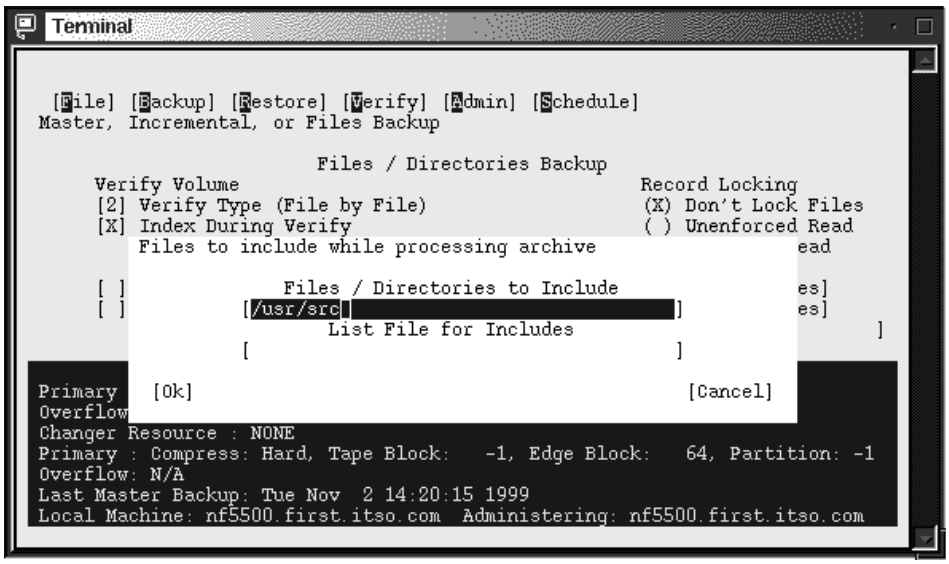


Figure 193. Selecting source for backup

3. In the Files / Directories to Include field, type in the files or directories you want to back up. In our example we want to make backups of the directory /usr/src. Select **OK** to continue. You will see a window similar to Figure 194.

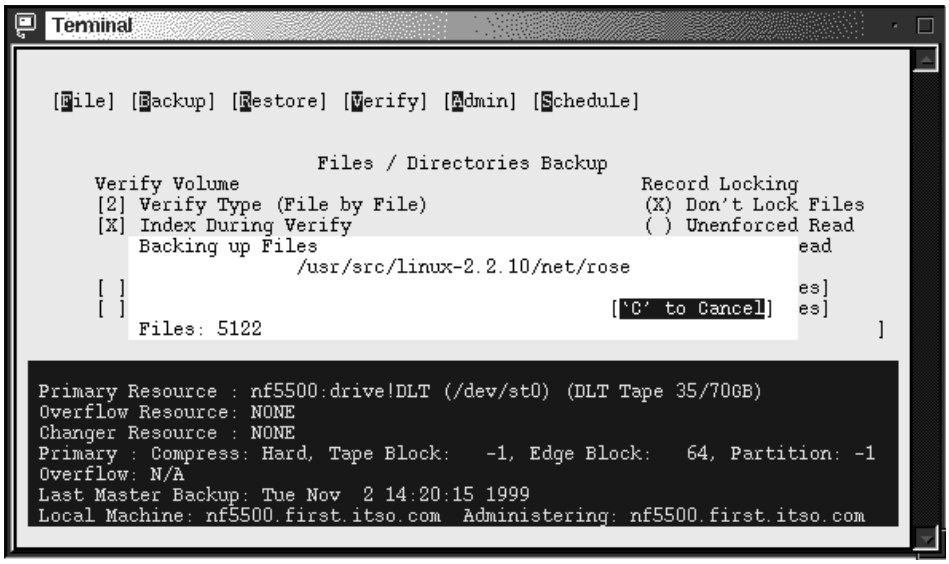


Figure 194. Backup in progress

After the backup is finished you will see a window similar to Figure 195.

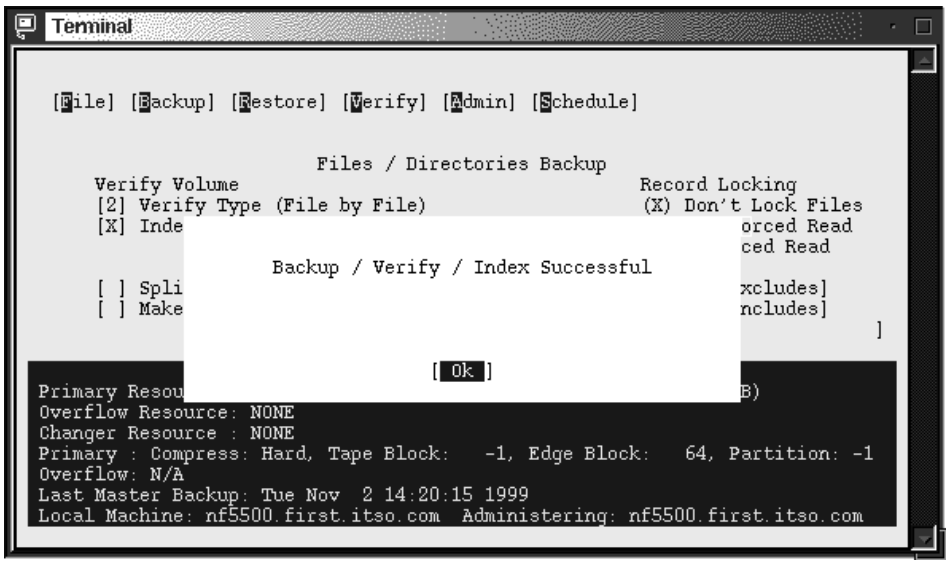


Figure 195. Backup completed

You will also see the backup report similar to Figure 196.

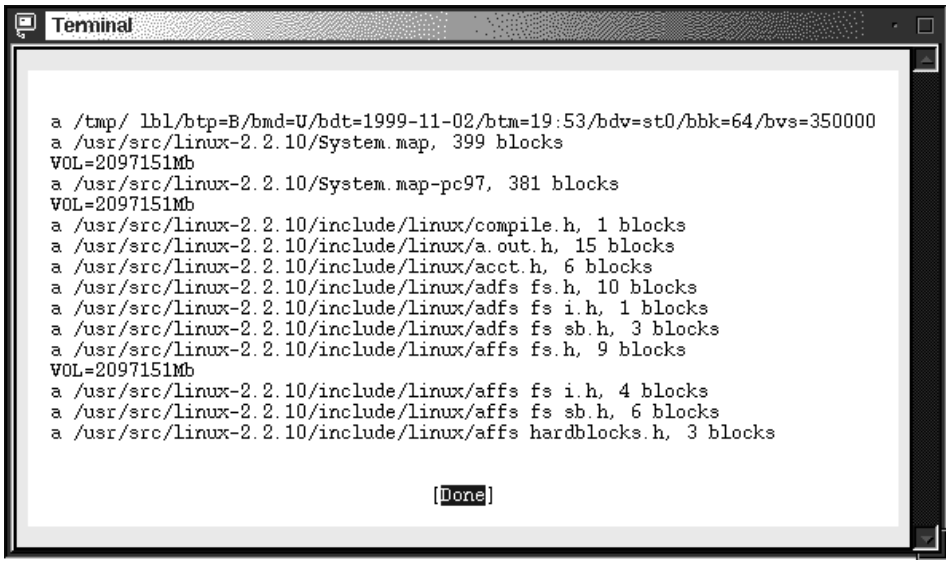


Figure 196. Backup report

You have just made your first backup and your files are safe now!

7.2.4 Restoring single files or directories

In this section we will show how to recover files from the backup. We are assuming that you are recovering files on the same server you made backups with the same user ID. You can perform recovery from the same utility as backups. Follow these steps to recover files:

1. Start the edgemenu program by executing the following command:

   ```
   edgemenu
   ```

   You will see a window similar to Figure 192. Select **Restore** and a window similar to Figure 197.

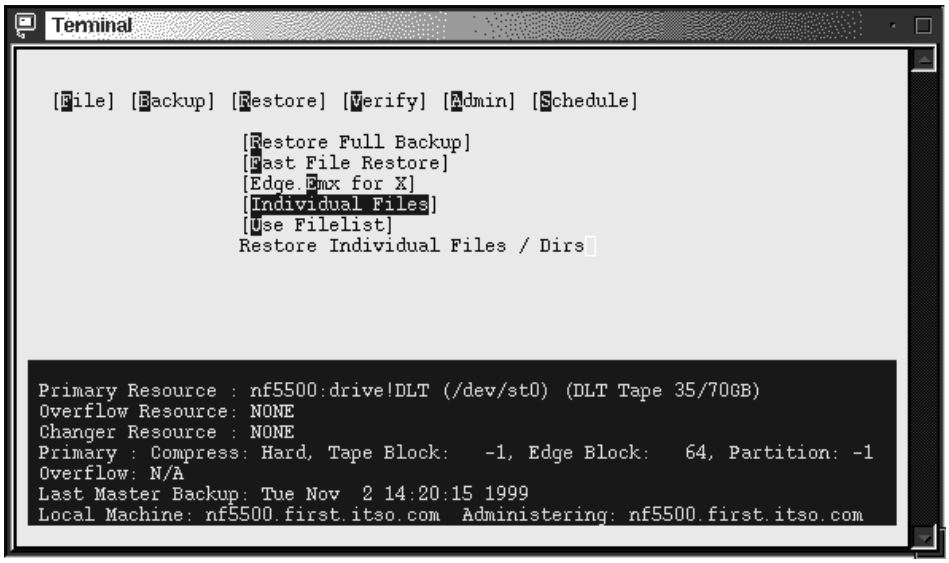


Figure 197. Starting the recovery

2. Select **Restore** > **Individual Files**, and you will see a window similar to Figure 193 on page 195.
3. Select the files or directories to restore. Select **OK** to continue, and you will see a window similar to Figure 198.

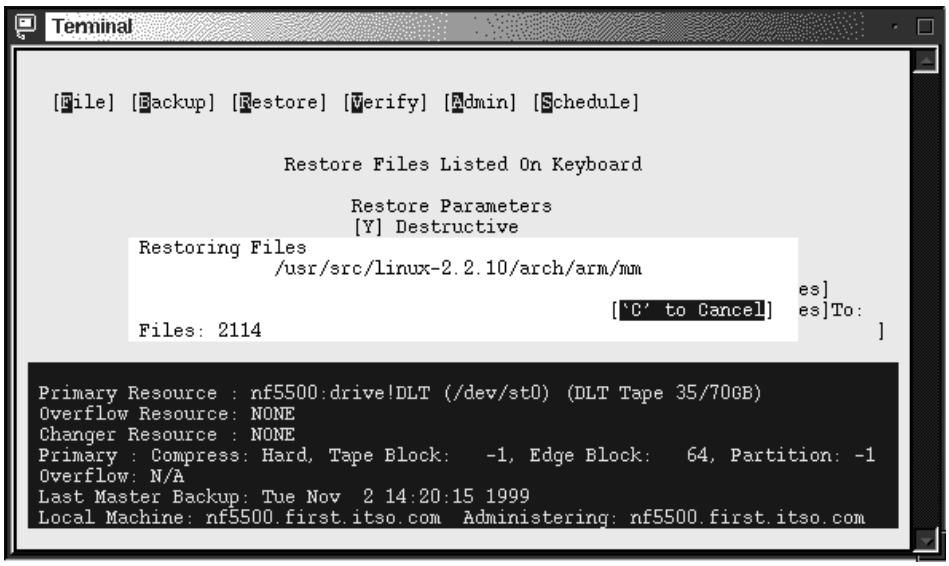


Figure 198. Recovery in progress

When the recovery is completed you will see a window similar to Figure 199.

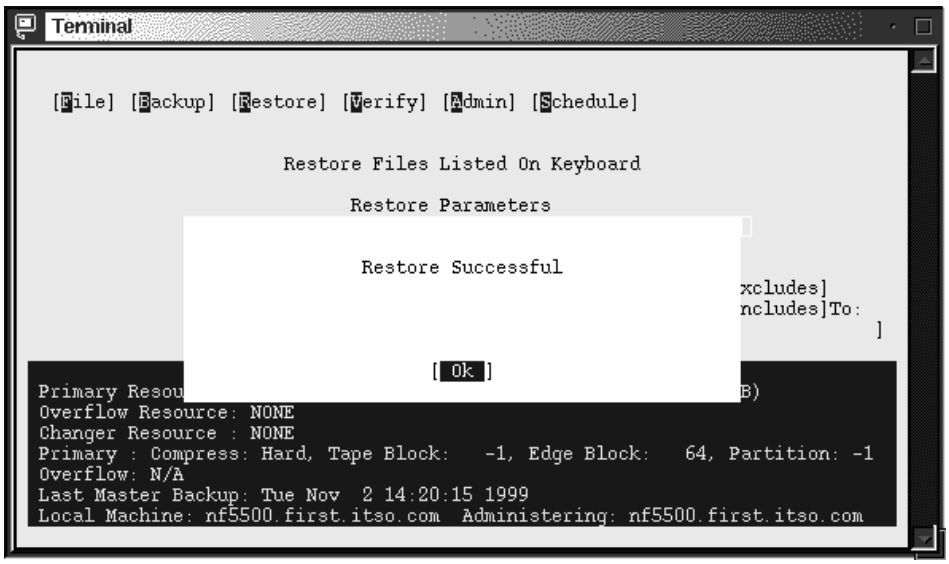


Figure 199. Recovery completed

Select **OK** to continue and you will see a recovery report similar to Figure 200.

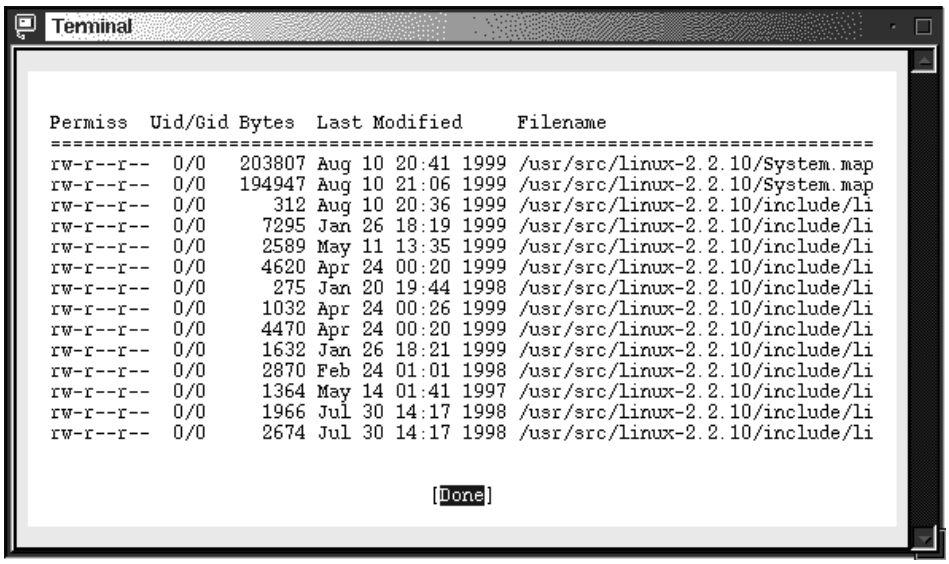


Figure 200. Recovery report

Your files were recovered successfully!

7.2.5 Master and incremental backups

Usually system administrators perform so-called master and incremental backups. The master backup is a backup of all files on the system. Incremental backup is a backup of only those files that have changed from the last master backup. When you need to restore your data, restore the master backup and the last incremental backup. BackupEDGE can perform different types of incremental backups. Refer to the BackupEDGE manual for the explanation of them. Master and incremental backups can be performed from the edgemenu utility.

To perform a master backup follow these steps:

1. Start the edgemenu program by executing the following command:

   ```
   edgemenu
   ```

   You will see a window similar to Figure 192 on page 195.

2. Select **Backup** > **Master Backup,** and you will see a window similar to Figure 201.

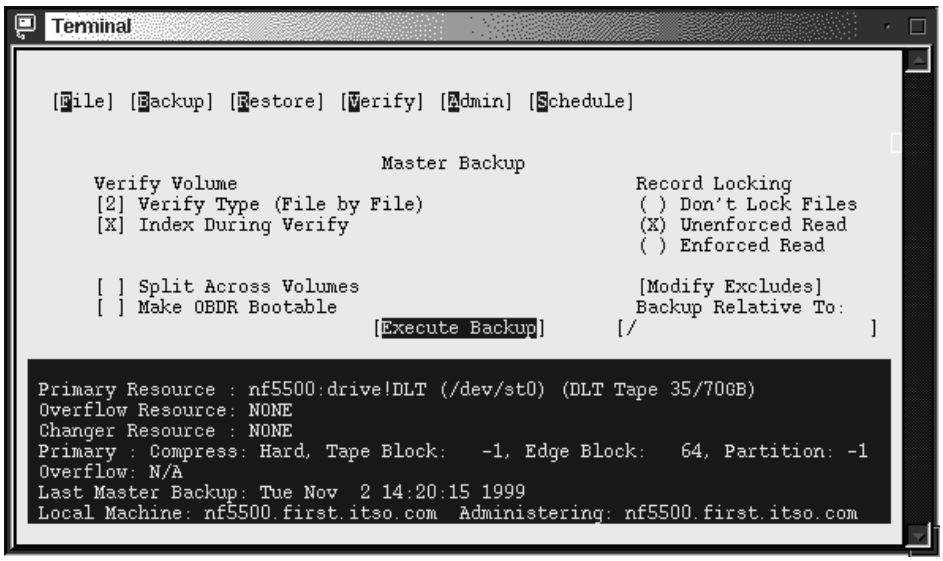


Figure 201. Starting the master backup

3. Choose the options you want and select **Execute Backup** to start the backup. You will see a window similar to Figure 202.

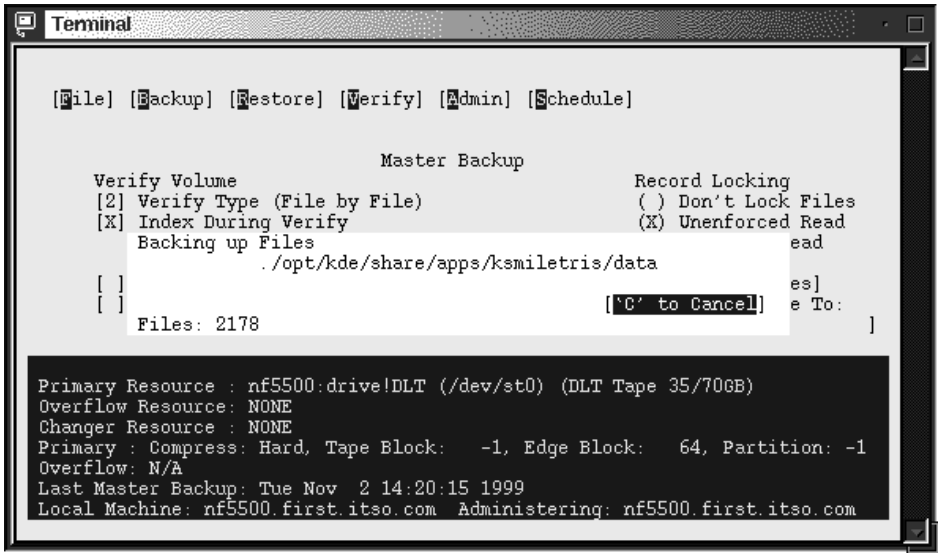


Figure 202. Master backup in progress

When the backup is finished you will see a window similar to Figure 203.

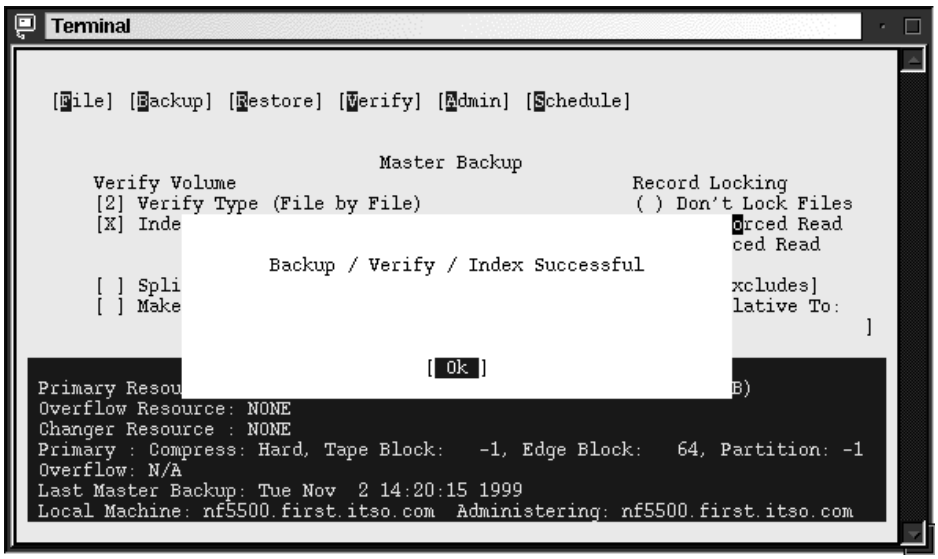


Figure 203. Master backup completed

Select **OK** to finish the operation, and you will see a backup report similar to Figure 204.

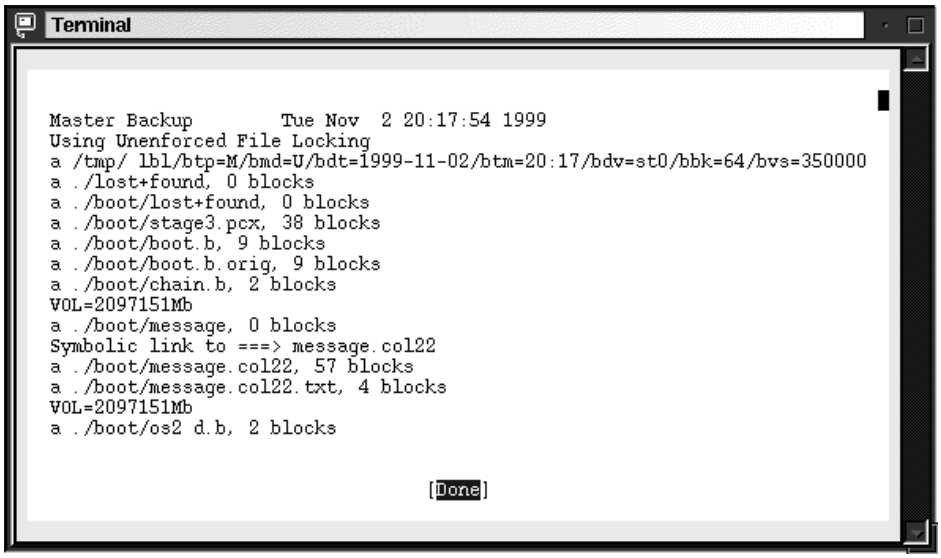


Figure 204. Master backup report

To perform incremental backups select **Backups** > **Incremental Backup.** Then follow the instructions in the window; they are similar to the ones for master backup.

7.2.6 Restoring master and incremental backups

To restore master and incremental backups you can use the edgemenu utility. When you start the utility and choose **Restore** you will see a window similar to Figure 205.

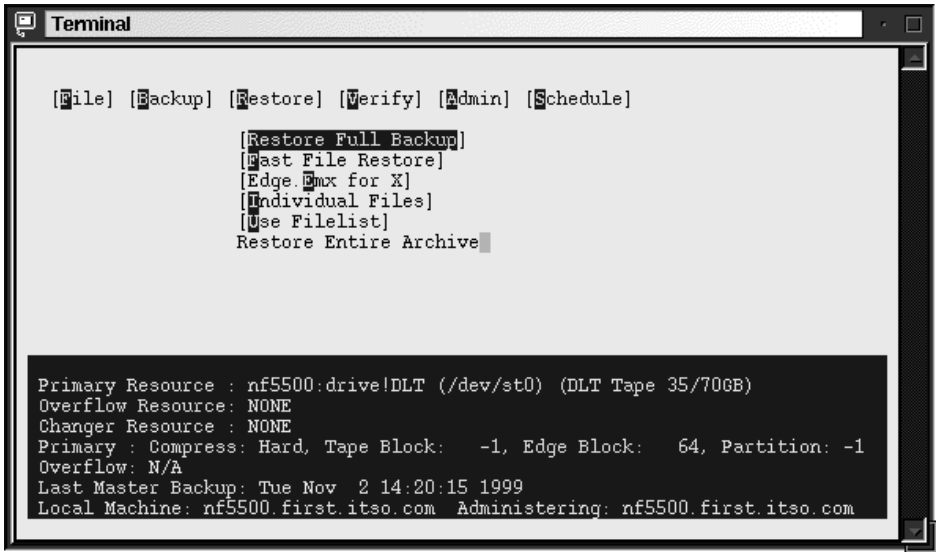


Figure 205. Starting restore full backup

Select **Restore > Restore Full Backup** and you will see a window similar to Figure 206.

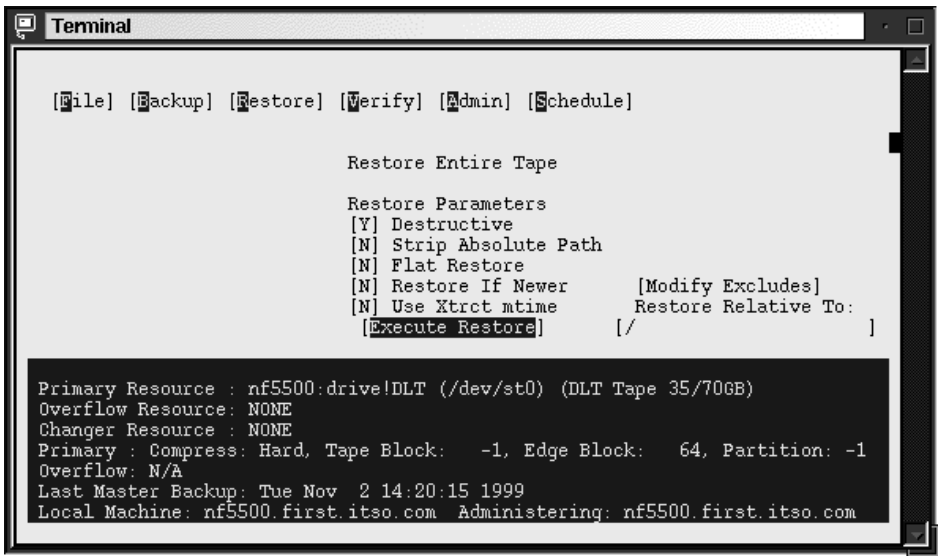


Figure 206. Full backup restore options

Choose your options and select **Execute Restore** to start restoring files.

7.2.7 Performing scheduled backups

To perform scheduled backups, you can use the edge.nightly utility included with BackupEDGE. To start this utility, execute the command:

```
/usr/lib/edge/bin/edge.nightly
```

But before you can use scheduled backups, you need to define them. To do this follow these steps:

1. Start the edgemenu.
2. Select **Schedule > Nightly Scheduling.** You will see a window similar to Figure 207.

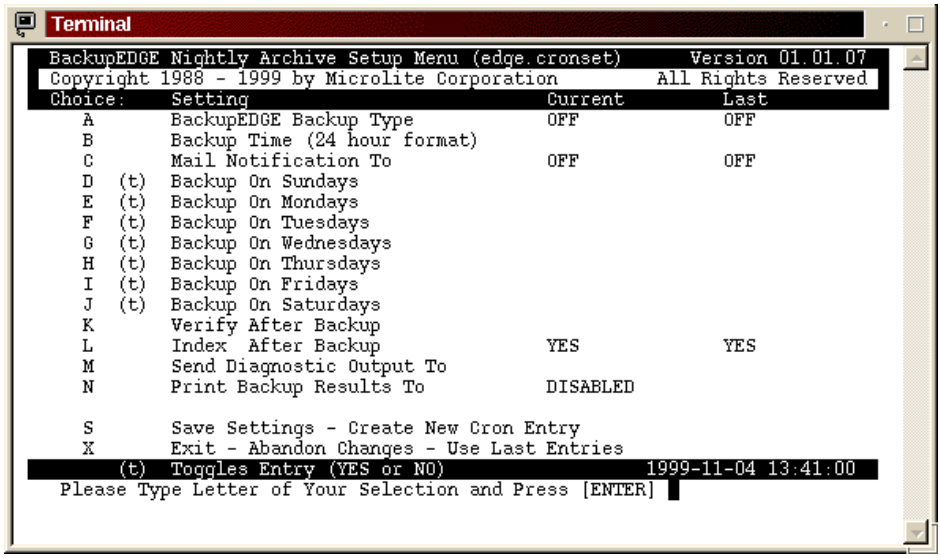


Figure 207. Schedule setup

3. Here you can define the schedule for your backups. You need to define the type and time of the backup. To define the type of the backup select **A** and press Enter, and you will see a window similar to Figure 208.

Figure 208. Defining the type of backup

4. Specify the type of backup you want to perform. In our example we selected **M** for master backup. You will be returned to the main window.

Note

You cannot mix master and incremental backups. If your master backup fits on one tape cartridge, we recommend that you do a master backup daily. If your master backup will not fit on one tape cartridge, do a manual master backup once a week and do incremental backups daily.

5. Next you need to specify the time of everyday backup by selecting **B** and pressing Enter. You will see a window similar to Figure 209.

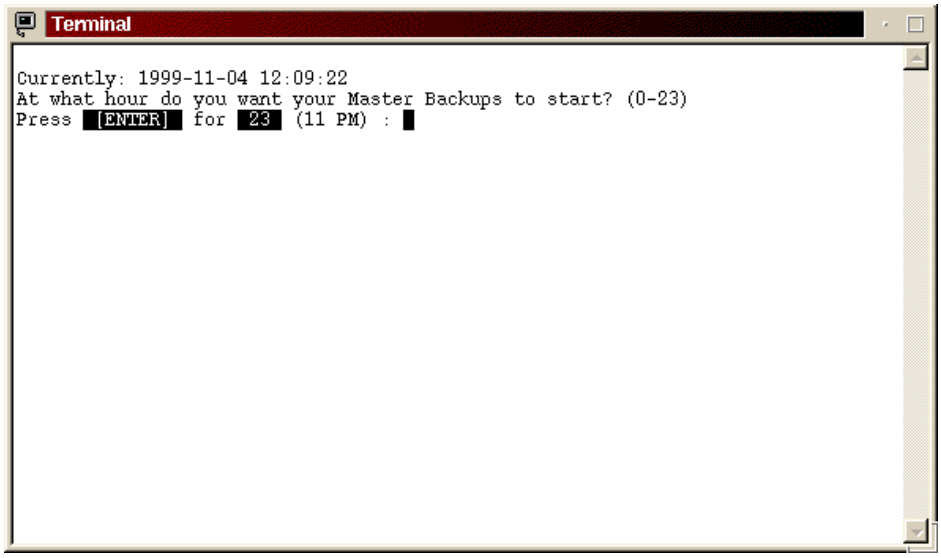


Figure 209. Setting the time

6. Define the time for your backups. You will see a window similar to Figure 210.

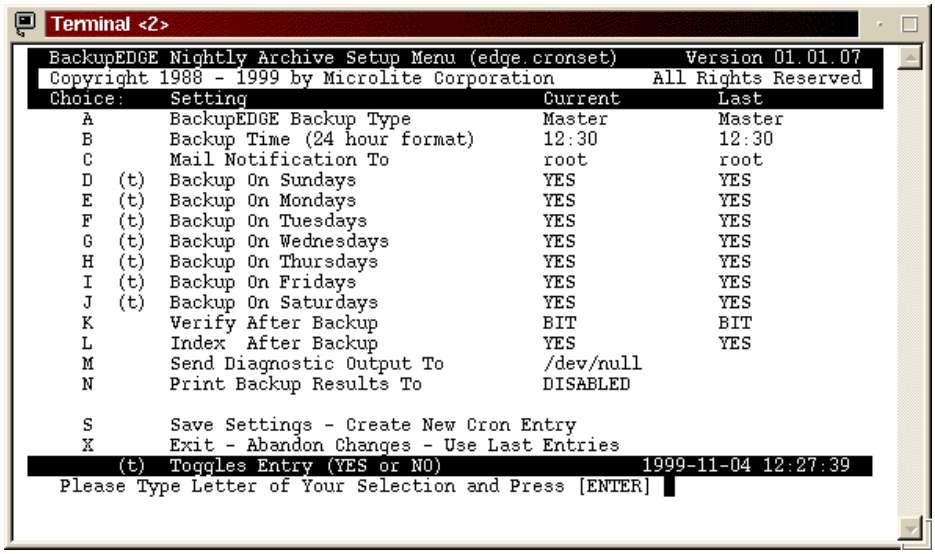


Figure 210. After schedule definition

7. Select **S** and press Enter to save the settings. The configuration program will create an entry in the cron database for executing the edge.nightly utility. From now on, cron will execute the backup utility as you defined in the previous steps.

Note

Before you start using scheduled backups, check if you need to copy the file /usr/lib/edge/bin/S88egde to the /etc/rc.d/rc2.d directory. This script will clear all zombie PIDs from the edge.nightly on the system restart.

You can also start edge.nightly from your own scripts. When you start it from a command line or a script, you have to be logged in as root. After edge.nightly is started it will perform an immediate backup.

7.2.8 Configuring the tape devices

Any time after installation you can define or change your backup device. To accomplish this follow these steps:

1. Start the edge.resmgr resource manager by executing the command:

   `/usr/lib/edge/bin/edge.resmgr`

   You will see a window similar to Figure 211.

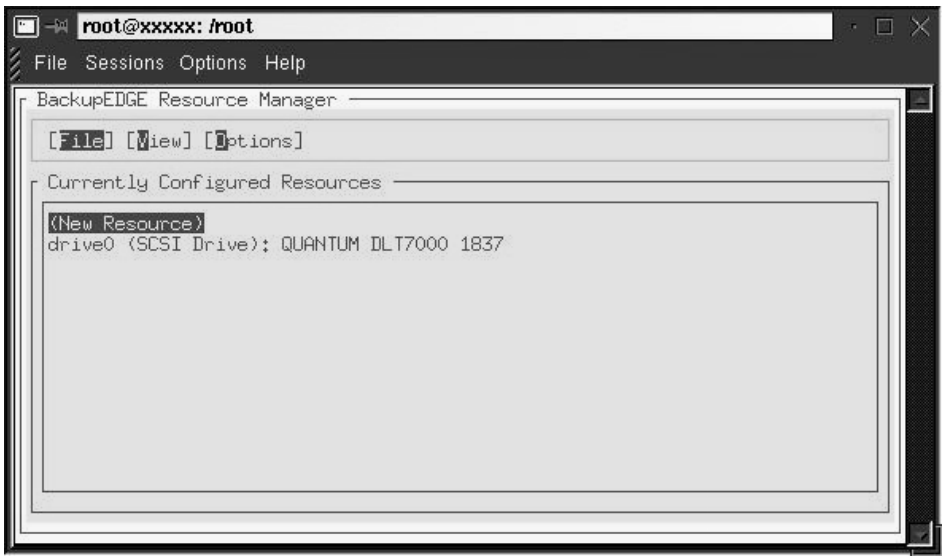


Figure 211. Starting the resource manager

2. Select **New Resource** and press Enter. You will see a window similar to Figure 212.

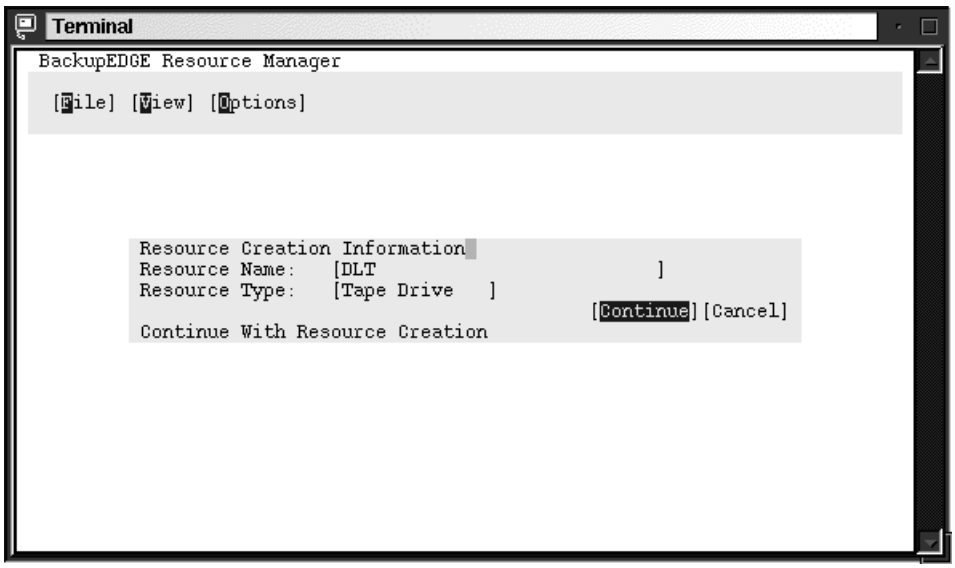


Figure 212. Defining the resource name

3. Type in the resource name and select a resource type. Select **Continue** to go on. You will see a window similar to Figure 213.

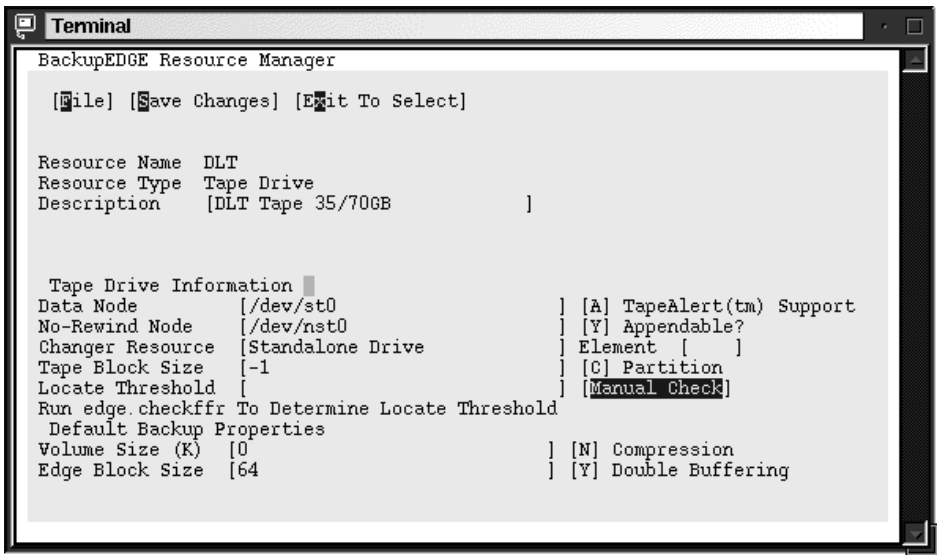


Figure 213. Parameters for the tape

4. Type in the description, data node and no-rewind node. In our example, the data node is `/dev/st0` and no-rewind node is `/dev/nst0`. You can leave all other fields as default.
5. Select **Manual Check** to define other parameters automatically. You will see a window similar to Figure 214.

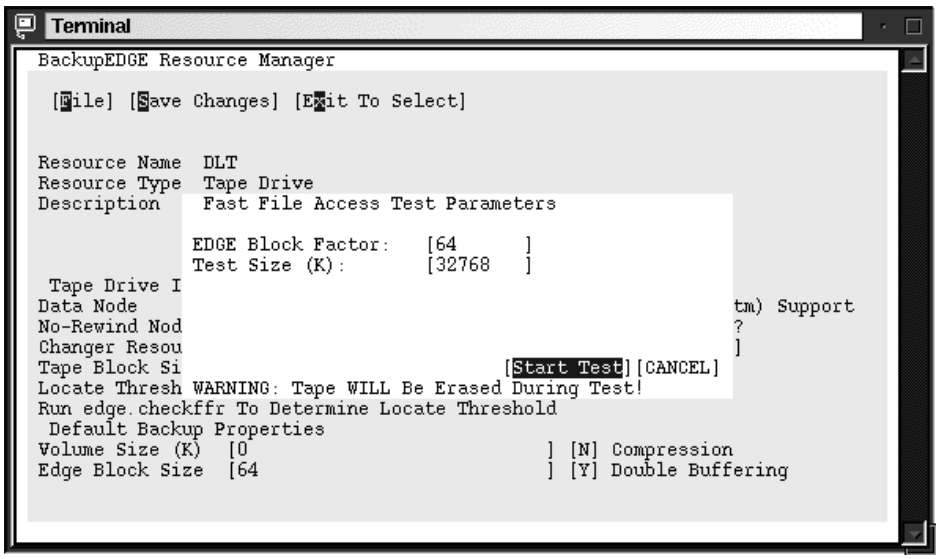


Figure 214. Setting the parameters for tests

6. Here you can select the block factor and the test size. Select **Start Test** to continue. You will see a window similar to Figure 215.

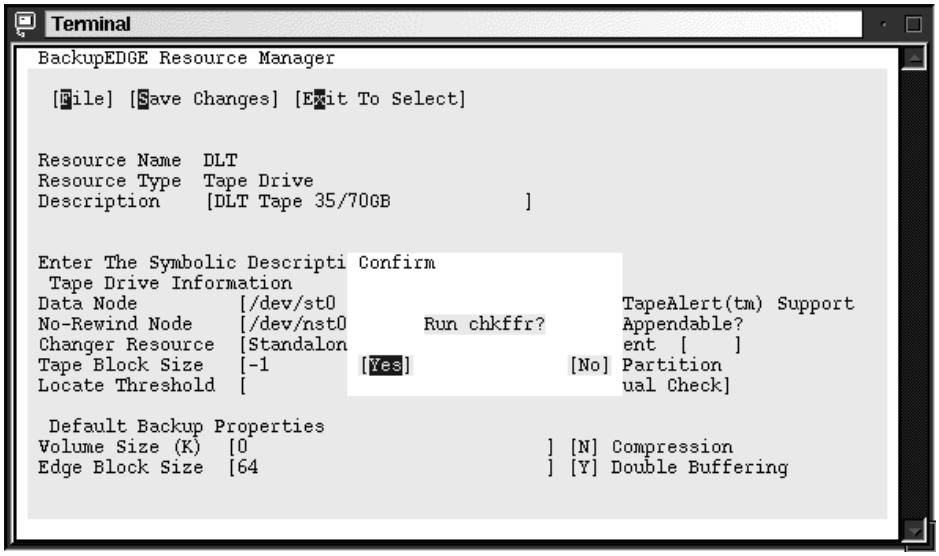


Figure 215. Starting the test

Stop

Performing this test will destroy all data on the tape.

7. Select **Yes** to continue. You will see a window similar to Figure 216.

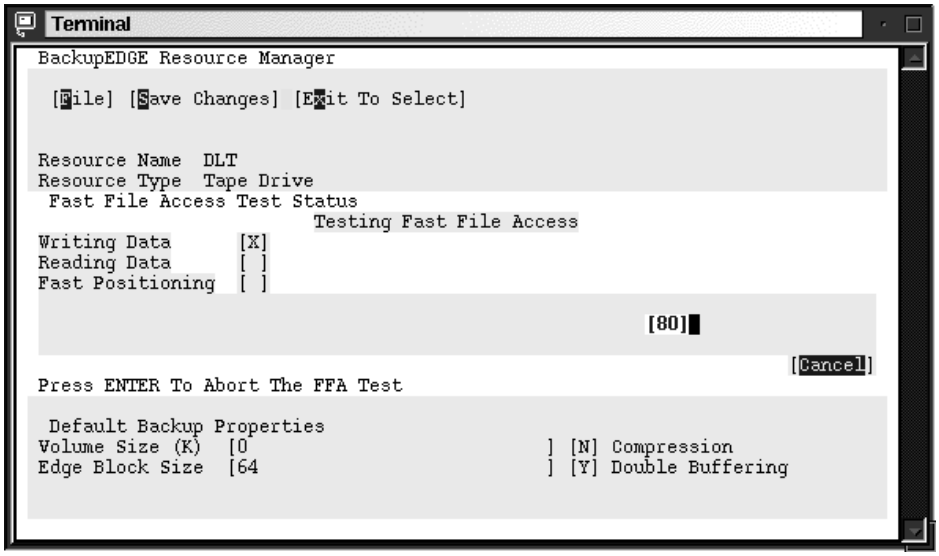


Figure 216. Performance test

After the test is done you will see a window similar to Figure 217.

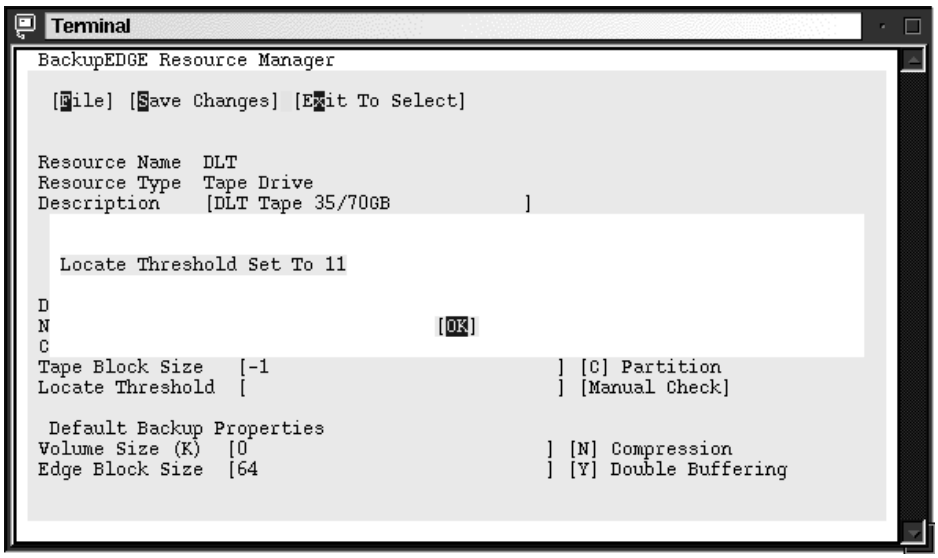


Figure 217. Threshold value

8. After the test is done you will see the proposed value for the threshold. Click **OK** to continue. You will be back in the parameters definition window similar to Figure 214 on page 210. Here you need to define four more parameters:
   - Volume Size
   - EDGE Block Size - the default size is 64 for a 32 KB buffer
   - Compression
   - Double Buffering - with multiple buffers you can increase the backup speed
9. Save the changes by selecting **Save Changes.** You will see a window similar to Figure 218.

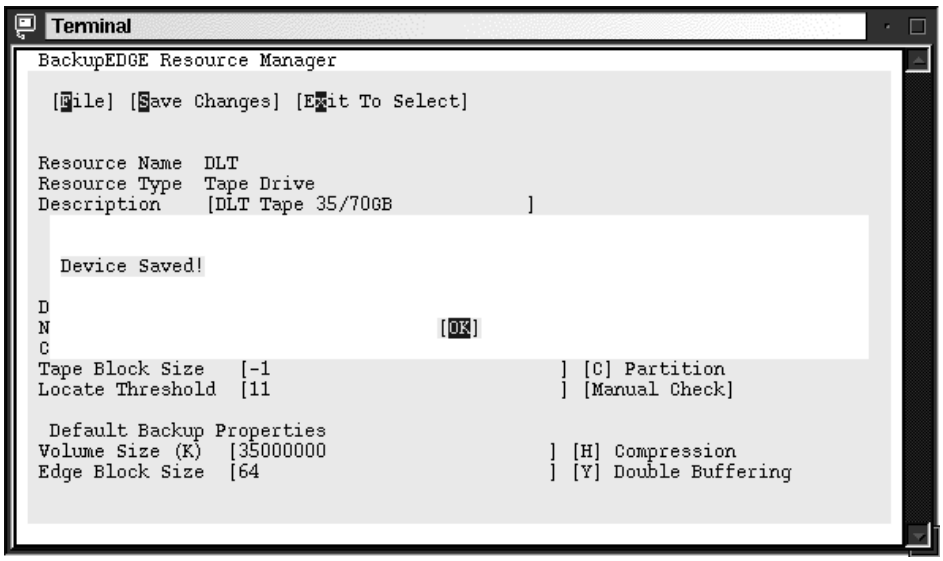


Figure 218. Saving the device definitions

7.2.9 Defining the devices for making backups

Any time after installation when you configured your backup hardware device, you can change which device the backup software uses for each user performing backups. If you are logged in as root, you will define devices for the root user. Usually this is the only user doing backups on the system. Follow these steps to enter the resource manager for backup:

1. Start the edge.config configuration menu by executing the command:

   `/usr/bin/edge.config`

   You will see a window similar to Figure 219.

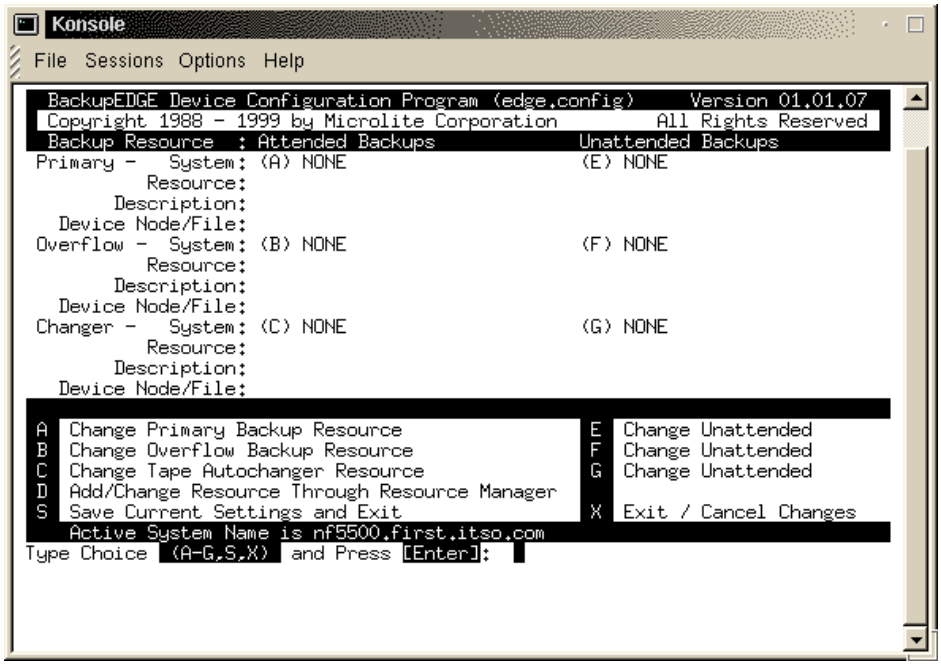


Figure 219. Device Configuration

2. Here you need to define the devices for attended and unattended backups.
3. Type in A and press Enter to define the device for attended backups. You will see a window similar to Figure 220.

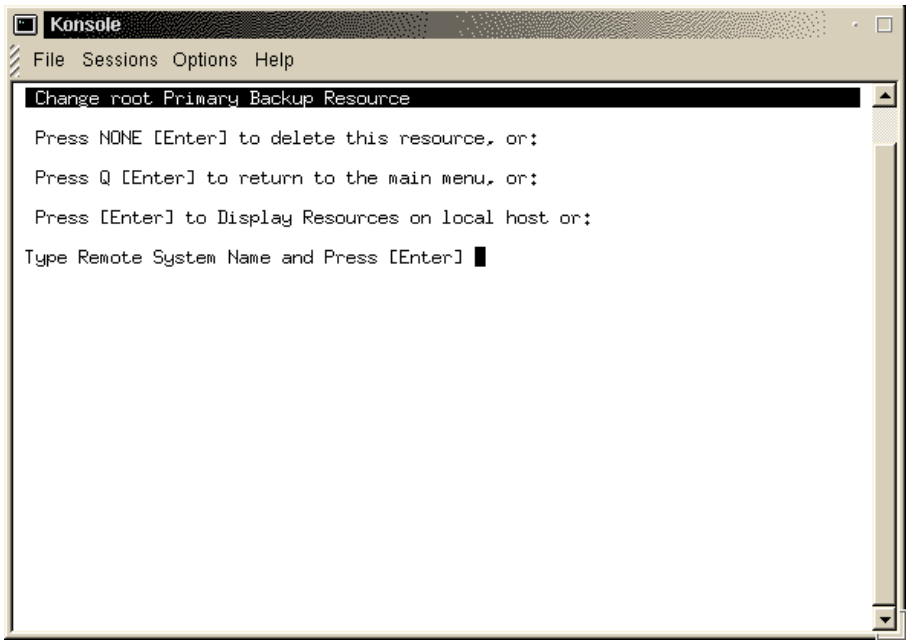


Figure 220. Selecting the device for backup

4. Press Enter to continue. In the next window you will see all defined backup devices. Type in the device you want and press Enter to continue. You will see a window similar to Figure 221.

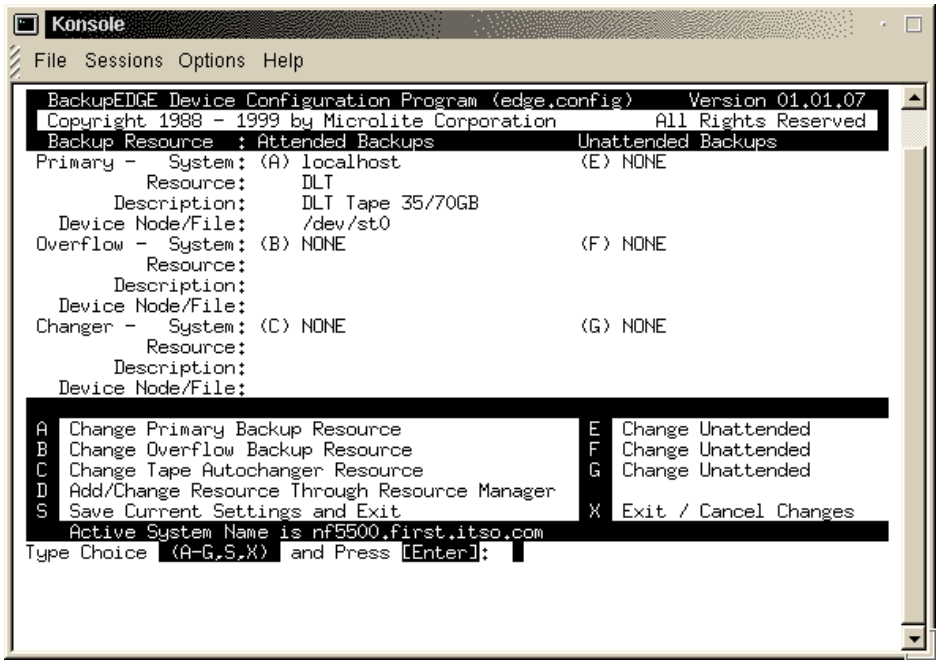


Figure 221. After definition of attended backup device

5. Follow the steps from 1- 4 for the unattended device also.

7.2.10 RecoverEDGE

By using the RecoverEDGE tools you can create emergency recovery diskettes to rebuild your system in the case of disaster. RecoverEDGE handles the details of reconstructing your FDisk, divvy, and/or slice tables, rebuilding your file systems and restoring your data, even if your hard drive size has changed. RecoverEDGE uses your live system backups, so there is no need to shut down your system in order to protect it. You can even restore your system over the network.

With RecoverEDGE restoring the system is very easy. To recover the system you should follow these tasks:

1. Identify and correct the cause of the failure.
2. Boot from the RecoverEDGE disks.
3. Reconfigure your file systems.
4. Restore your backups.
5. Shut down and reboot.

6. System is ready to use.

Note

RestoreEDGE uses your master and incremental backups for recovery, so the accuracy of the data depends on these backups.

7.2.10.1 Creating the RecoverEDGE boot disks

Before you can use RecoverEDGE for disaster recovery you should build a set of boot disks. To create the boot disks follow these steps:

1. Start the utility for creating the RecoverEDGE boot diskettes:

   ```
   /usr/bin/re2
   ```

   or go to **Admin>Make RecoverEDGE Media** in the menu.

   You will see a window similar to Figure 222.

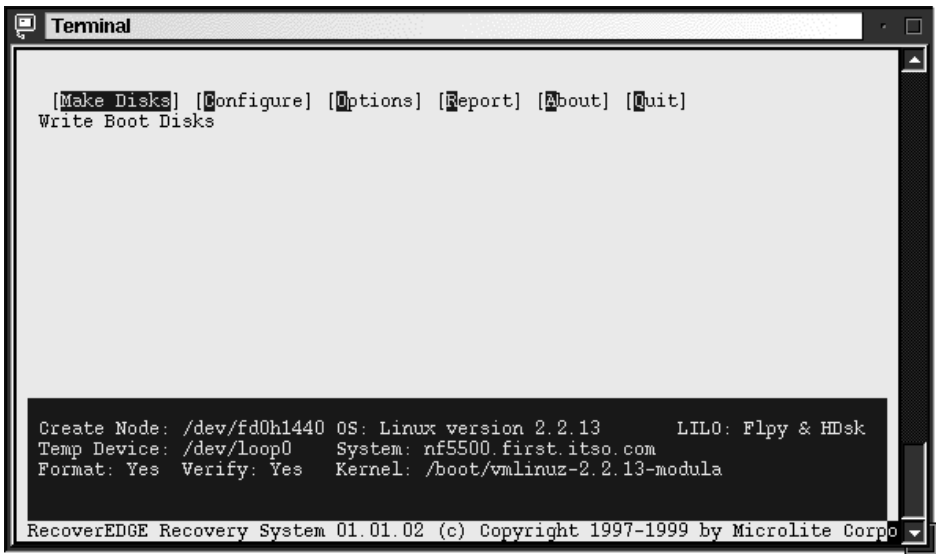


Figure 222. RecoverEDGE utility

2. Select the **Configure** option and press Enter, and you will see a window similar to Figure 223.

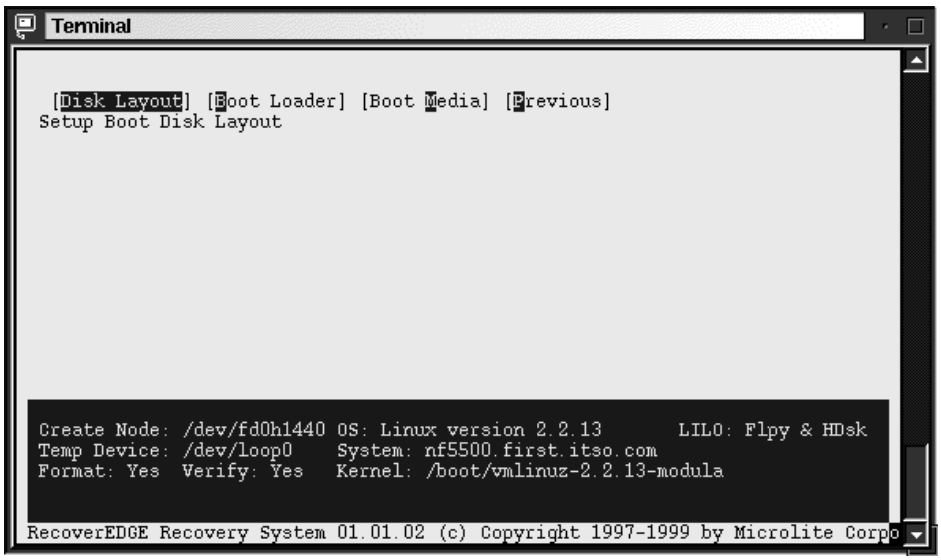


Figure 223. Configure menu

3. Select the **Disk Layout** option and press Enter, and you will see a window similar to Figure 224.

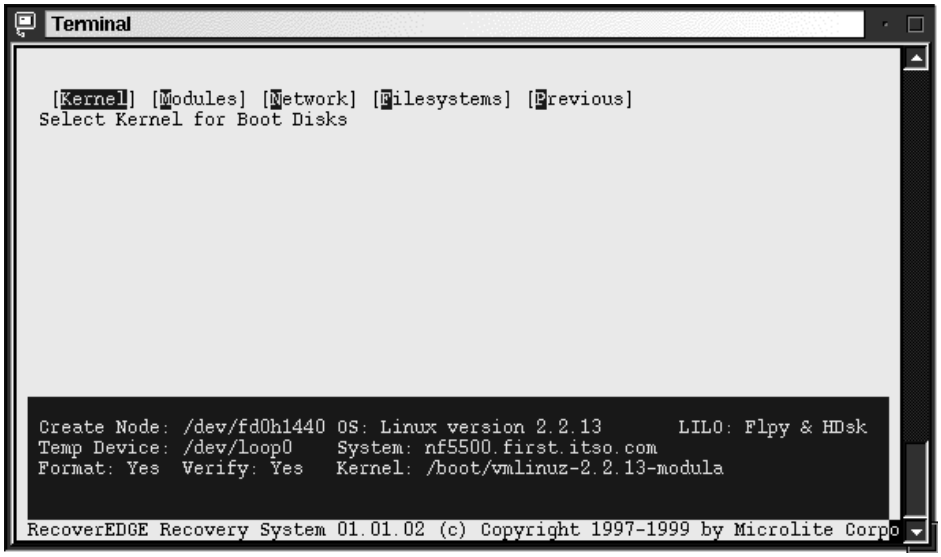


Figure 224. Disk layout menu

4. Here you can configure the kernel, modules, network and the file systems for your RecoverEDGE boot disks. Select the **Kernel** option and you will see a window similar to Figure 225.

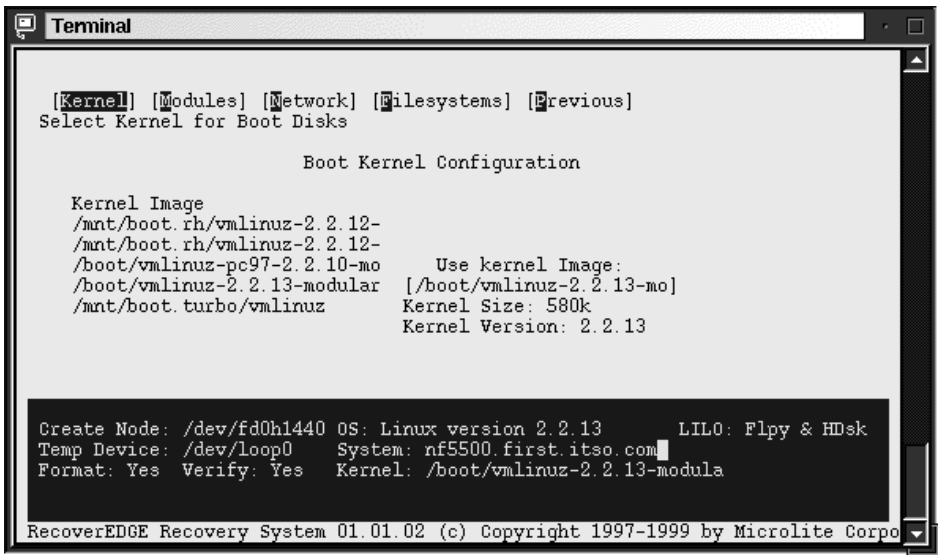


Figure 225. Kernel options

Here you define which kernel will be used for creating the diskette.

5. Return to the previous stage and select **Modules** and press Enter, and you will see a window similar to Figure 226.

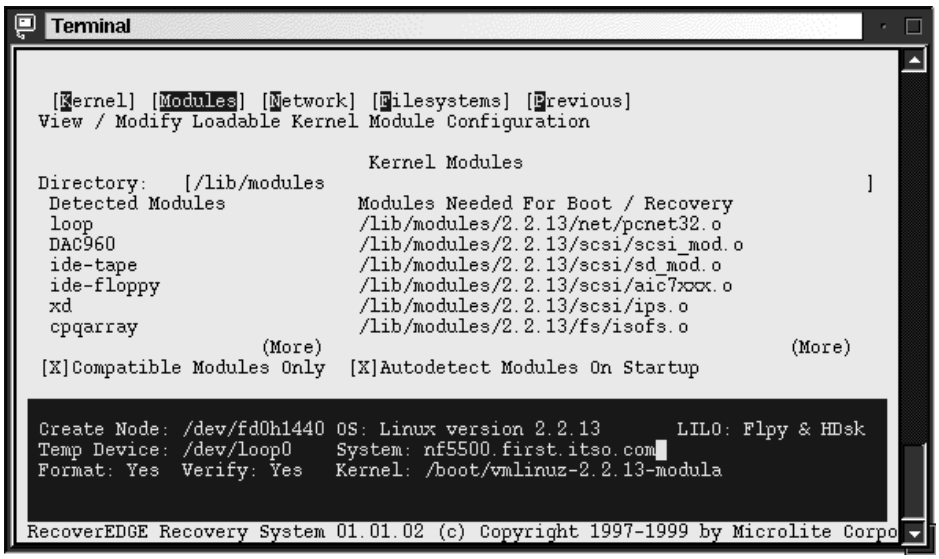


Figure 226. Modules options

Here you define which modules will be used for building the initial RAM disk for the recovery system. In the Directory field you can specify the path to the modules that corresponds to the kernel you defined for booting. If you choose the option **Autodetect Modules on Startup,** RecoverEDGE will load currently loaded modules.

Note

Do not forget to include the module for the tape drives.

6. Return to the previous stage and select **Network** and press Enter, and you will see a window similar to Figure 227.

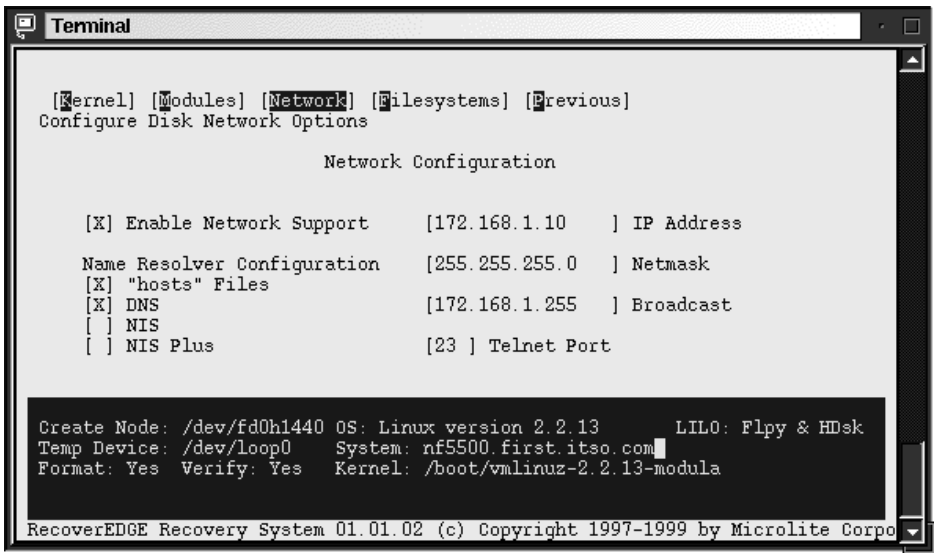


Figure 227. Network options

Here you define you network setup in case you will restore the system from a tape device on the network. You do not need this if you have a locally attached tape.

7. Return to the previous stage and select **Filesystems** and press Enter, and you will see a window similar to Figure 228.

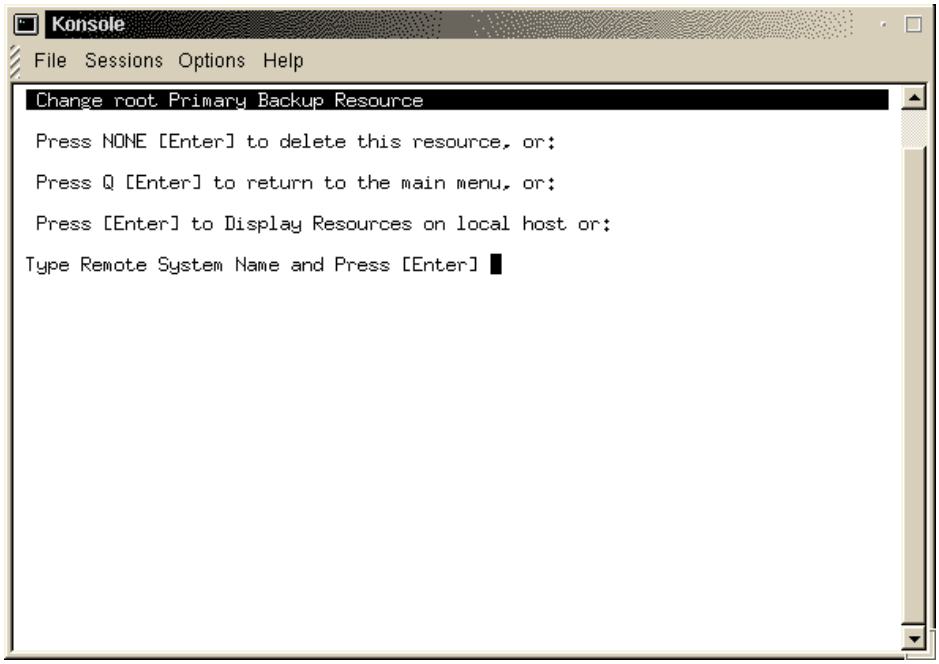


Figure 228. Filesystems options

Here you define which mounted file systems will be recovered.

8. Return to the configuration panel and select the **Boot Loader** option and press Enter. You will see a window similar to Figure 229.

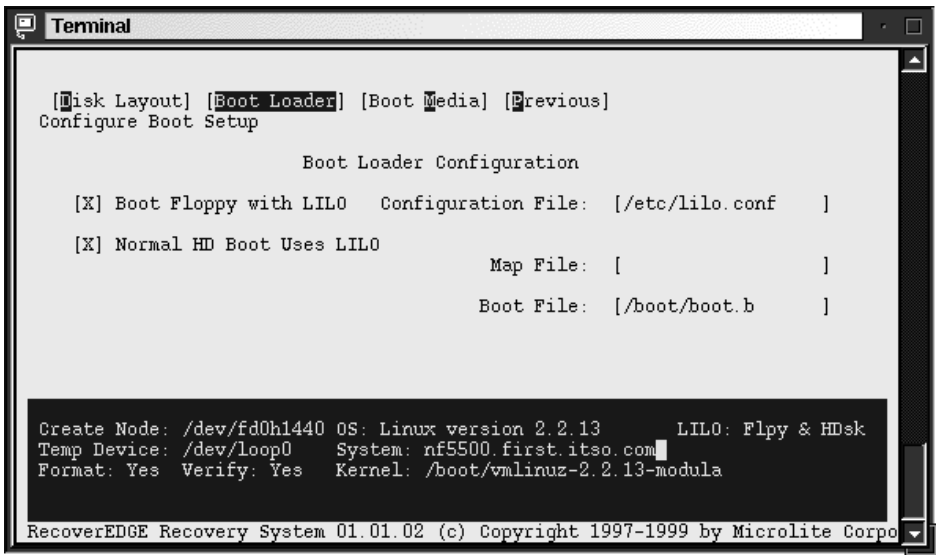


Figure 229. Boot Loader options

Here you define options for the Boot Loader.

9. Return to the configuration panel and select the **Boot Media** option and press Enter. You will see a window similar to Figure 230.

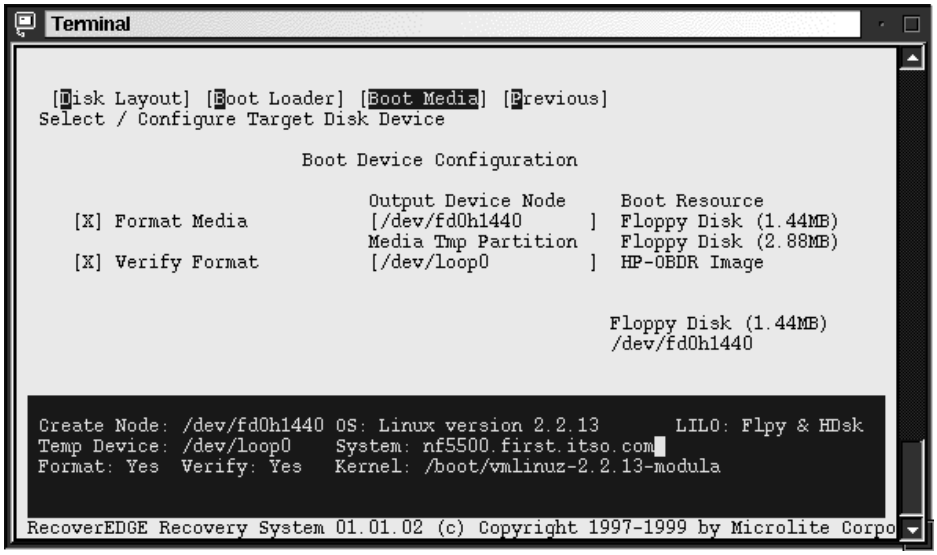


Figure 230. Boot Media options

Here you define how the boot diskettes will be created.

10. After you configured all settings return to the main window and select **Make Disks.** You will be prompted to insert three diskettes.

> **Note**
>
> If you get an error that diskettes cannot be created, the probable cause is that images are too big. Try to reduce the number of loaded modules or even make the special kernel just for this purpose, throwing out all unnecessary things.

After the diskettes are created you are ready to deal with disaster on your system. But before this really happens, try to boot from these diskettes and verify if your tape device is recognized.

7.2.10.2 Verifying the RecoverEDGE boot diskettes

To verify the diskettes, boot from the first diskette and follow instructions on the window. When the system is started you will get the RecoverEDGE main menu. Select **Utilities** > **Tape Drive**.

In the Tape Device Node field, you see the defined tape device. Go to the Test Tape Drive field and test your tape device. If the test is successful your recovery set is ready to use.

7.2.10.3 Recovering from a total crash

To recover from a disaster crash follow these steps:

1. Resolve all hardware problems.

> **Note**
>
> Before restoring the system, initialize the Master Boot Records of all disk drives.

2. Boot the server from the first RecoverEDGE boot diskette.
3. When you are prompted to insert the root diskette, insert the second RecoverEGDE boot diskette. After the diskette is loaded, RecoverEDGE will start and you will see a window similar to Figure 231.

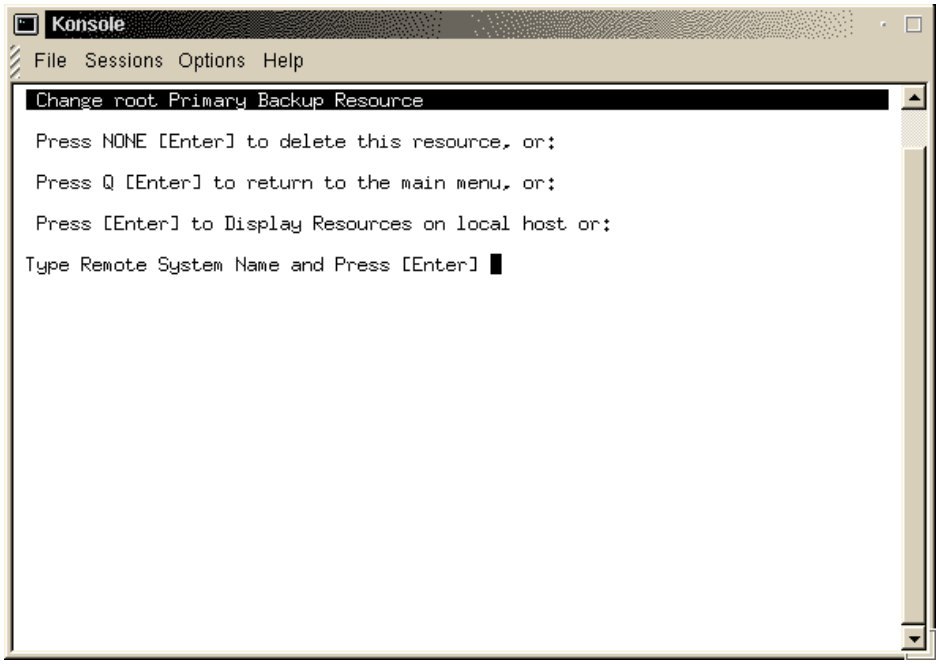


Figure 231. RecoverEDGE initial window

4. Select **Restore** > **One Touch**. Follow the instructions on the window to complete the recovery.

Note

For recovery you will use your master and incremental backups.

5. When all files are backed up, press a key to get back to the main window. All the file systems will be then synchronized and LILO will be set up and executed.
6. Before you reboot, switch to a console 2 with Alt+F2 and execute the following commands to check the fstab file for correct entries for your system:

   ```
   mount /dev/sdb6 /mount
   cat /mount/etc/fstab
   ```

   In our example `sdb6` is our root partition. You should use your root partition here.

That is all there is to it. Your restored system is ready to use.

7.2.11 More information on Microlite products

For information on advanced features consult the *Microlite User's Guide* or the Microlite Web site at:

```
http://www.microlite.com
```

7.3 Arkeia

Arkeia is a complete client/server backup solution for Linux and other platforms. In this section, we will prepare the installation of Arkeia.

The requirements for the server:

- A 486 processor or higher
- 32 MB RAM
- 1 GB disk space
- SCSI adapter card
- SCSI tape drive
- TCP/IP services
- Linux 2.0 or higher

The requirements for the client:

- A 486 processor or higher
- 5 MB disk space

In the following sections we describe how to install, configure and use the Arkeia backup software.

7.3.1 Installing Arkeia

Arkeia is available in different package formats (tar, rpm) for different distributions either on CD or downloadable from Arkeia's Web site (follow the link `http://www.arkeia.com`) in the DOWNLOAD AREA. To install Arkeia, we recommend that you follow the installation procedure described in the *Installation and Quick Start Manual*. You can find this manual on the Arkeia-CD or download it from Arkeia's Web site.

On the Arkeia server, you must also install the client and the GUI package. These packages are required to configure the backup server. After the installation of the client and GUI packages, you can install the server package.

7.3.2 Configuring Arkeia

Before you can configure Arkeia, check whether the Arkeia backup server is running. To do this, enter:

```
ps -ef | grep -v grep | grep nlservd
```

on the system which should be used as your backup server. If you see a line like

```
root 488 1 0 09:06 ? 00:00:00 /usr/knox/bin/nlservd start
```

the backup server is running. To begin with the configuration of Arkeia, be sure, your have X-Windows running. Then enter on the command line:

```
Arkeia
```

You will see a dialog like Figure 232:

Figure 232. Arkeia initial window

The field for the server name is by default filled in with the name of the system you currently work with. You must change this field if you have installed the server component on another system.

The field for the login name is by default filled in with `root`. Change it if you have changed the name of the Arkeia administrator.

The field for the password is empty by default. You have to enter the password when you have changed the password. The main dialog window of Arkeia appears (Figure 233):

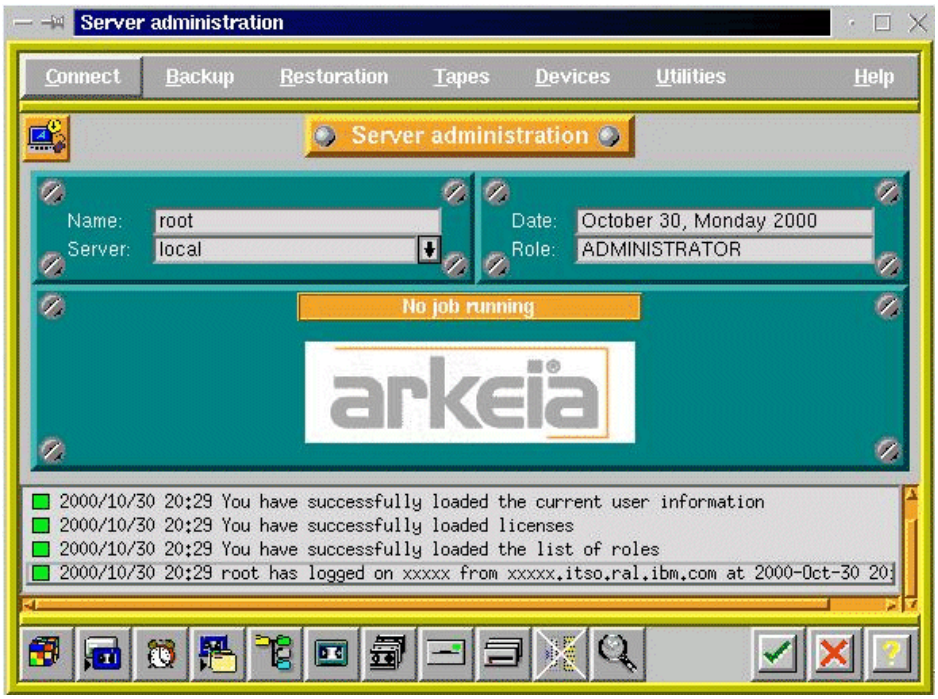


Figure 233. The Arkeia main dialog window

If you want a simpler layout of the window, go to **Utilities -> Setting** in the menu bar and modify the appearance of the windows. Click the **OK** button, save the new setting, and click the **OK** button again. Now, you will get a window similar to the window in Figure 234.

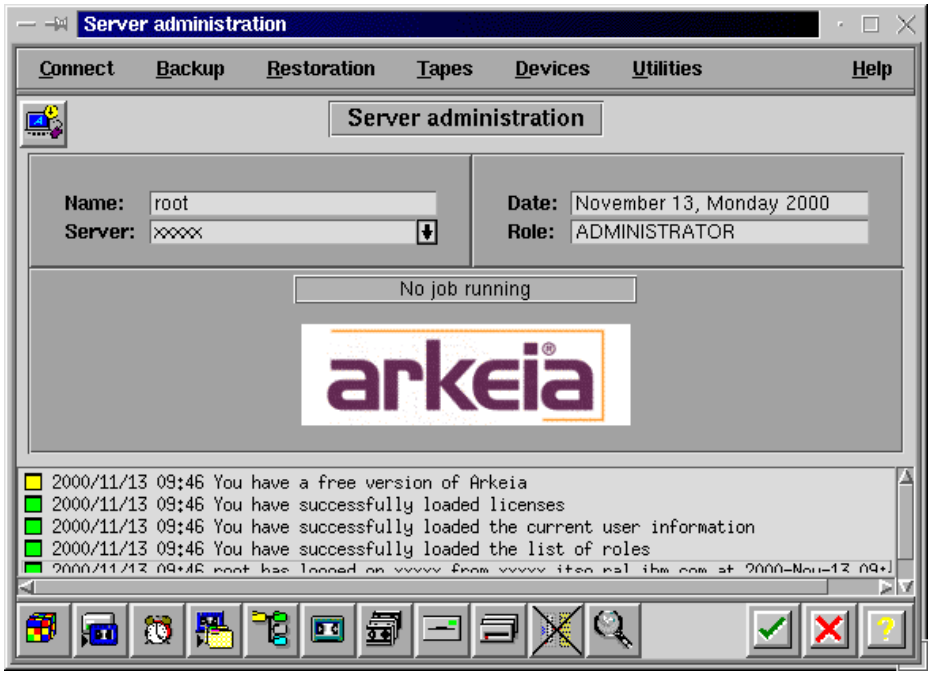


Figure 234. The new Arkeia main dialog window

At the bottom of the window you see push buttons shown in Figure 235:

Figure 235. Bottom part of main window

The meaning of these buttons is, from left to right:

- Refresh job
- Interactive backup
- Periodic backup
- Restoration
- Savepacks
- Tapes management
- Pools management
- Drives management
- Drivepacks
- Libraries management
- Backup done

- OK button. Clicking this button opens a new Welcome dialog.
- Cancel button. Click this button to leave Arkeia.
- Help

Before you can begin with your first backup, you must carry out the following configuration steps:

- Pool management
- Tape management
- Drives management
- Drivepacks management
- Savepacks management

Let us start with tape pool management. Click the pools management button on the bottom of the main dialog or click **Tapes -> Pools management** on the menu. The Pools management window appears as in Figure 236:

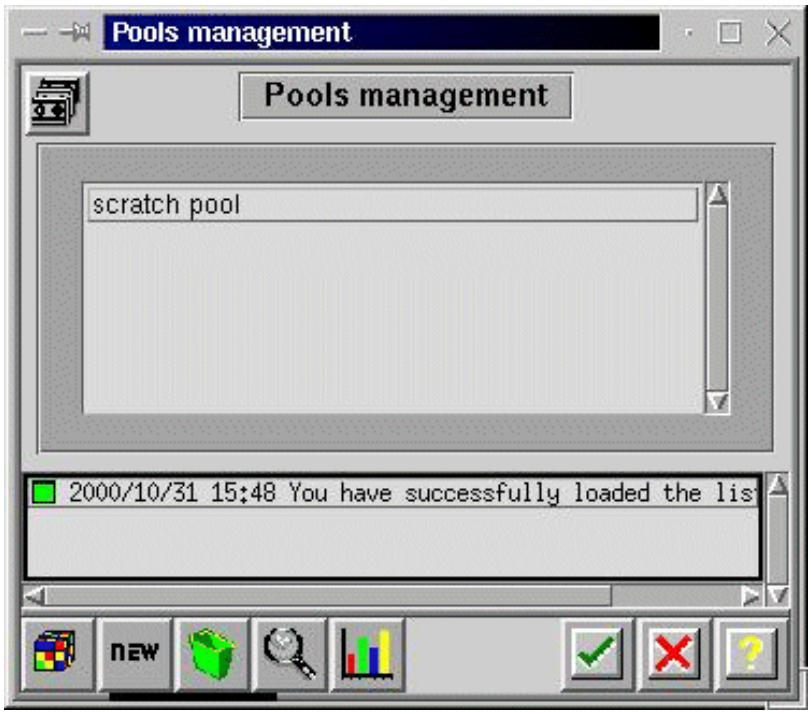


Figure 236. Pools management main dialog window

The scratch pool exists by default. To create a new tape pool, for instance for your backup tapes, click the **new** button. The Pool creation dialog appears as shown in Figure 237:

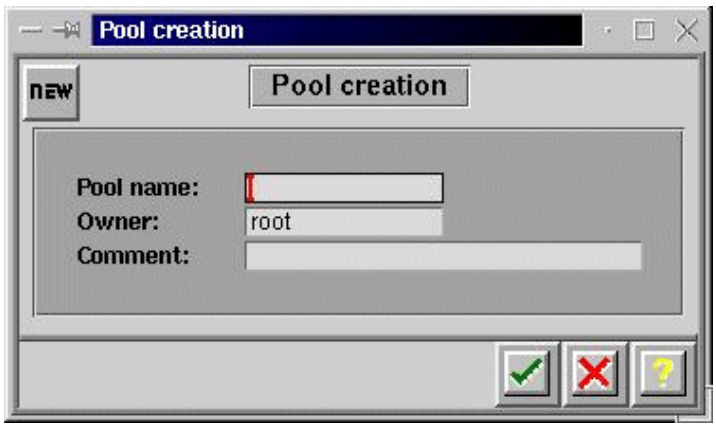


Figure 237. Pool creation window

Fill in the dialog fields with the appropriate information and click the **OK** button. The Pools management main window appears with the pool list updated as in Figure 238:

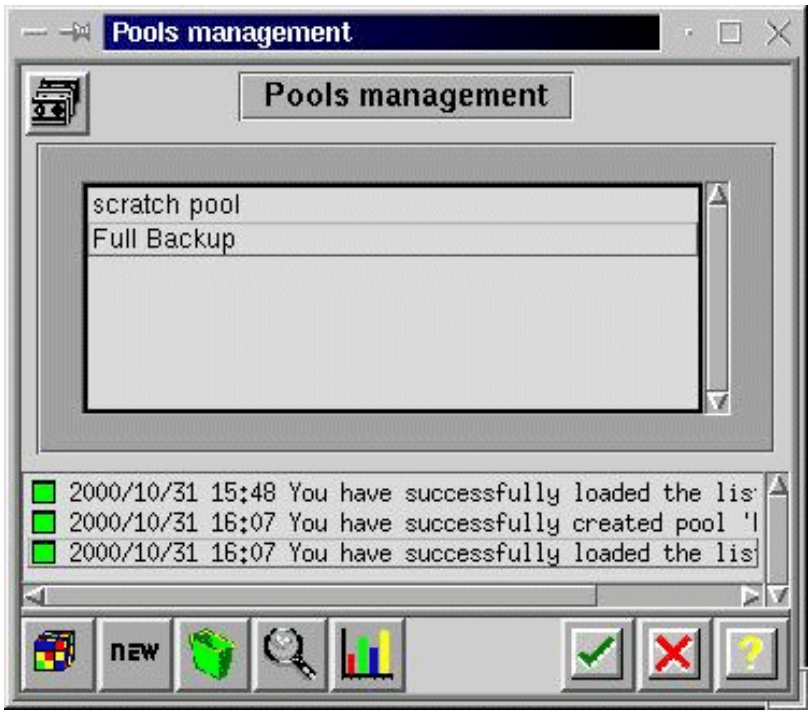


Figure 238. Pools management main window with updated pool list

To return to the main dialog, click the **OK** button. Now we can fill the Full Backup pool with tapes. To do this, click the tape management button or click **Tapes -> Tapes management** in the menu. The Tapes management main window appears (Figure 239):

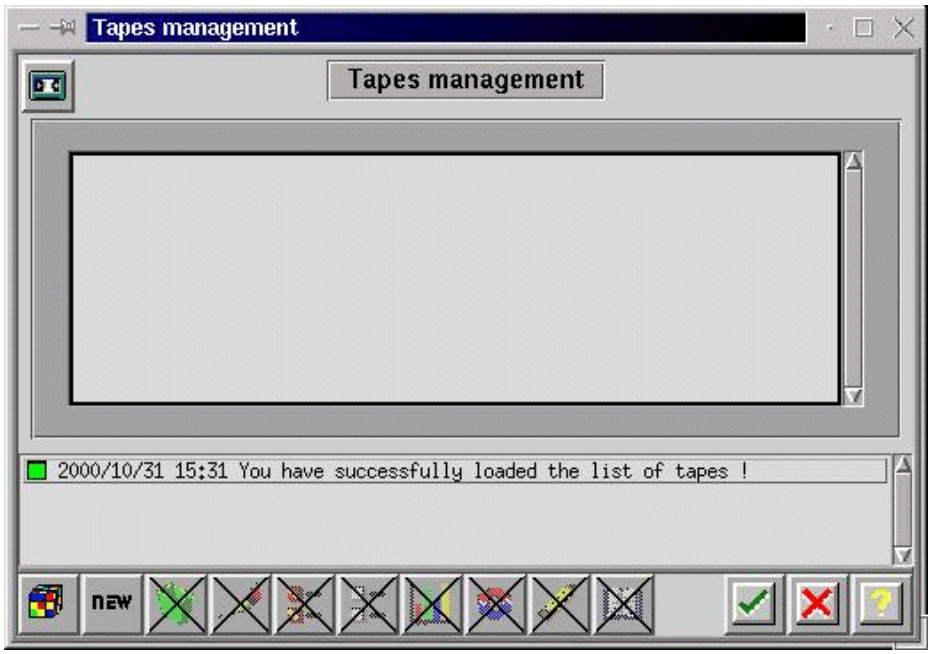


Figure 239. Tape management main window

Click the **new** button to enter new tapes (Figure 240):

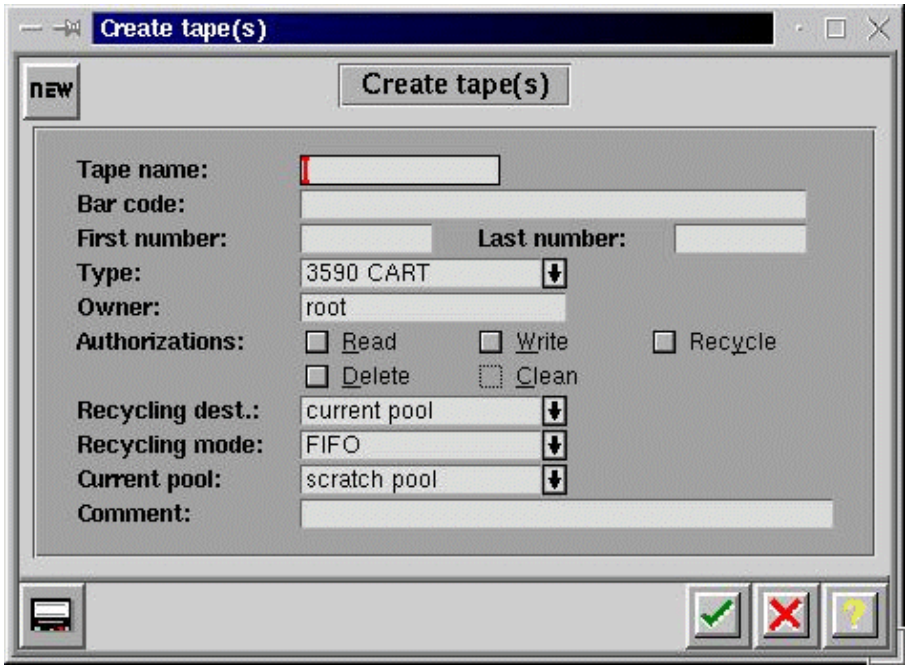


Figure 240. Create tape(s) window

The tape name consists of a fixed part and a variable part. The fixed part can be any text, while the variable part is a number. Enter the first part of the tape name, the first and the last number of the tapes to be used, and the tape type (DAT, DLT, etc.). Choose the pool these tapes should belong to and enter a comment in the comment line. Click the **OK** button to return to the tapes management main window. The Tapes management main window appears with the updated list of currently created tapes. Click the **OK** button in this window to return to the main window.

After the creation of tape pools and tapes, we can create drives and drive packs.

Drives must be created first. To do this, click the drives management button in the main window or click **Devices -> Drives management** in the menu. The Drives management window appears (Figure 241):

Figure 241. Drives management window

Click the **new** button to fill in the fields with the appropriate information. The fields Name and Rewind Device must be filled. Do not forget to choose the correct tape type in the Type field. To return to the Arkeia main window, double-click the **OK** button.

Now we can generate drivepacks. Click the drivepacks button or click **Devices -> Drivepacks** on the menu. The Drivepacks window appears (Figure 242):

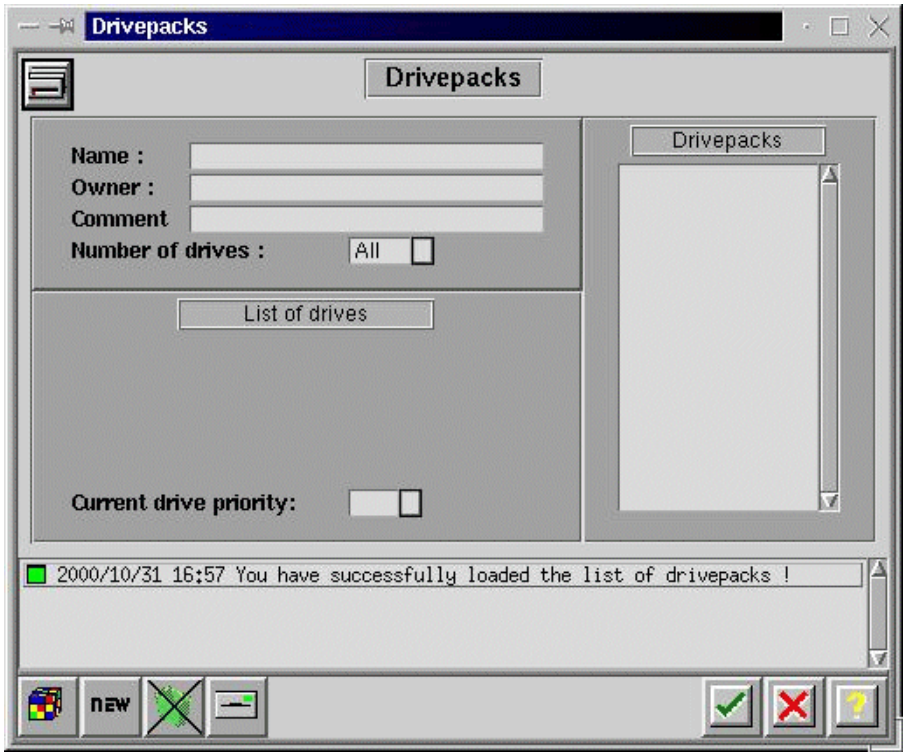


Figure 242. Drivepacks management window

Click the **new** button to fill in the fields. Fill in the Name field and choose one entry in the drives list and click the **OK** button to update the list of existing drivepacks on the right side of the window (Figure 243).

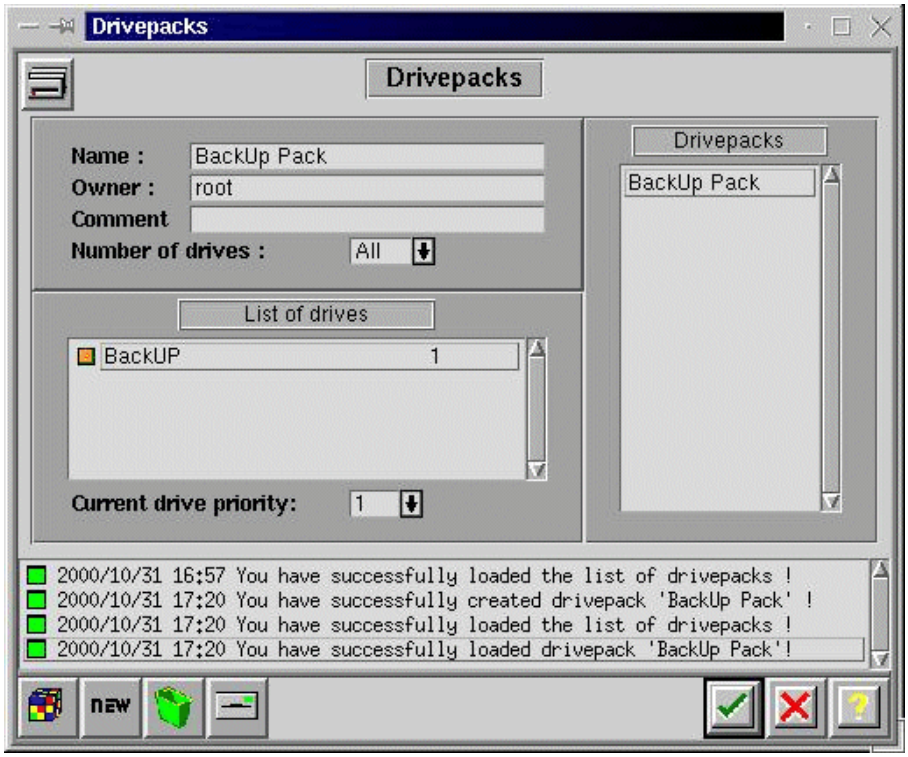


Figure 243. Updated drivepacks management window

Click the **OK** button again to return to the main dialog window.

The last step to be done before data can be saved is creating at least one savepack. You describe in savepacks which data should be saved. Different savepacks contain different sets of data to be saved.

To create savepack(s), click the savepacks button or click **Tapes -> Savepacks** on the menu. You will see a window like Figure 244:

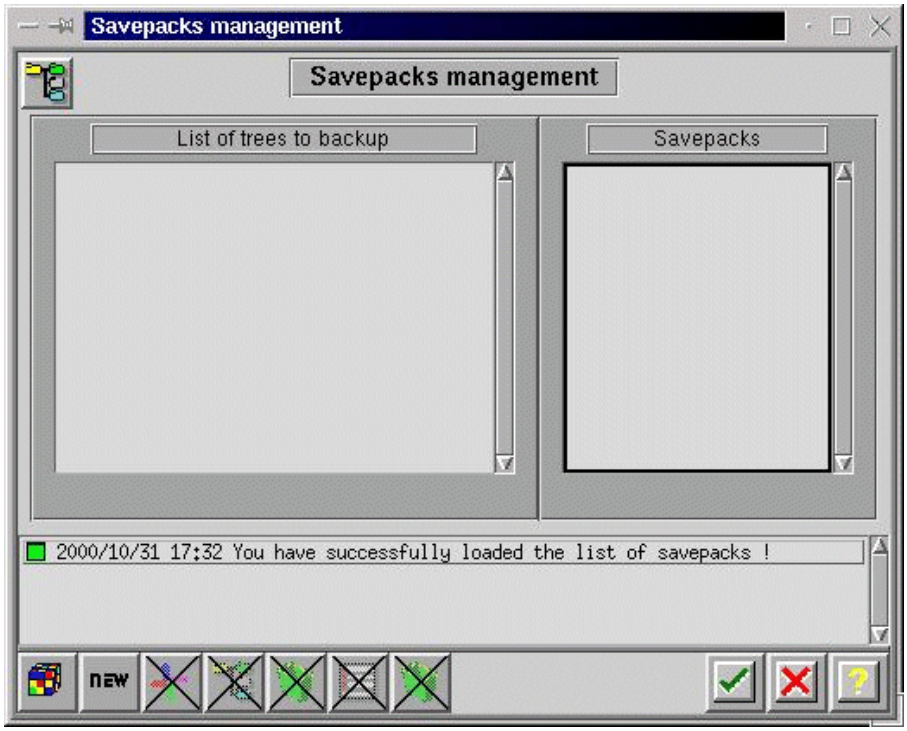


Figure 244. Savepacks management window

Click the **new** button to enter input mode. A window similar to Figure 245 appears.

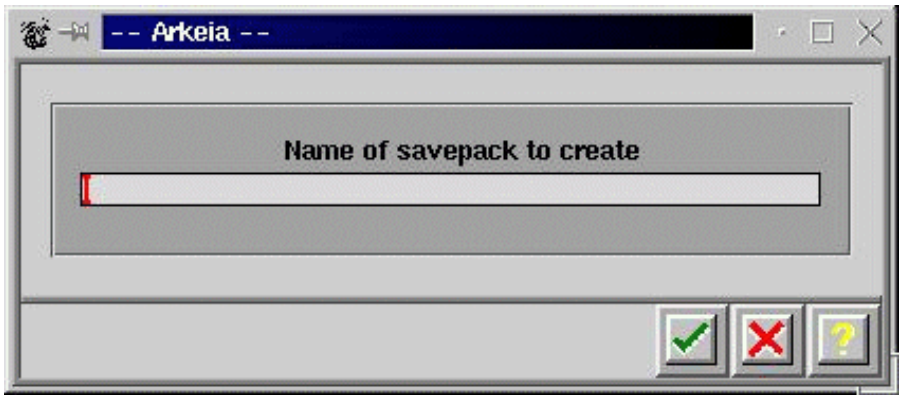


Figure 245. Window to create a new savepack

Enter the name of the new savepack and click the **OK** button to return to the updated Savepacks management window (see the list of savepacks on the right side of the window). A window like Figure 246 appears:

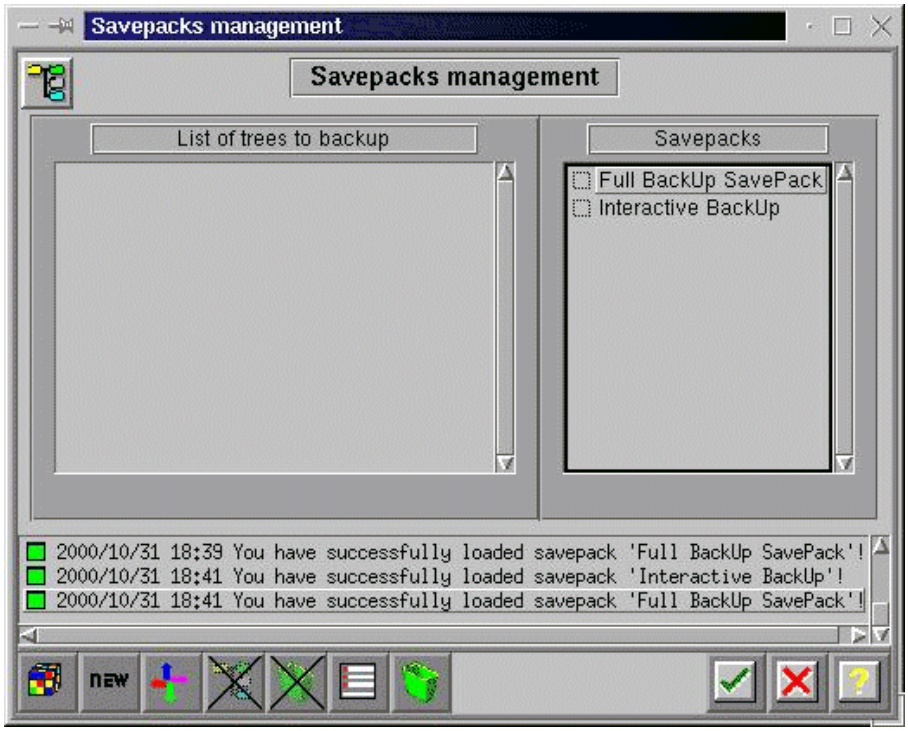


Figure 246. Updated Savepacks management window

Now, you select the data that should be saved in every created savepack. Move the cursor over the name of the savepack you want to select the data for and click the left mouse button. You can see the selected savepack.

Now, move the cursor over the list of trees to back up (left listbox of this window), click the right mouse button and select **Navigator** in the upcoming pull-down menu. You will see a window similar to Figure 247.

To navigate through the directory tree of a system shown in this window, move the cursor over the system you want to select and double-click the left mouse button. A window similar to Figure 248 appears.

Double-clicking the left mouse button over a directory symbol opens this directory and shows the content of this directory.

Clicking once with the left mouse button in the checkbox to the left of a directory name or file name toggles the select/unselect status of this item. All selected items will be inserted in the list of trees to back up for the selected savepack. If you select a directory, the checkbox changes the color totally. If you select only a selection of the items in a directory, the checkbox for this directory changes color only in the right half of the checkbox.

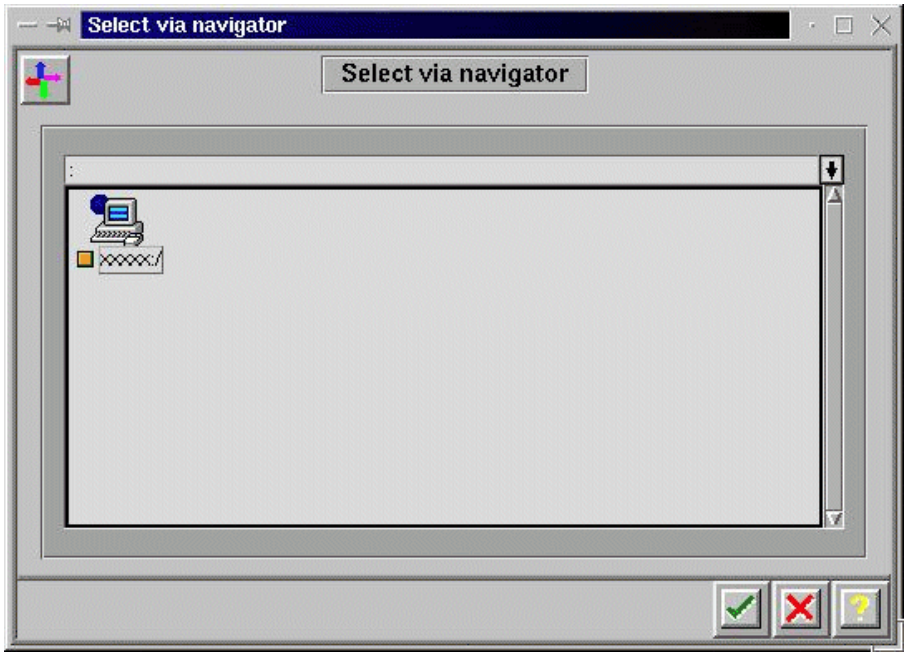


Figure 247. Navigator window

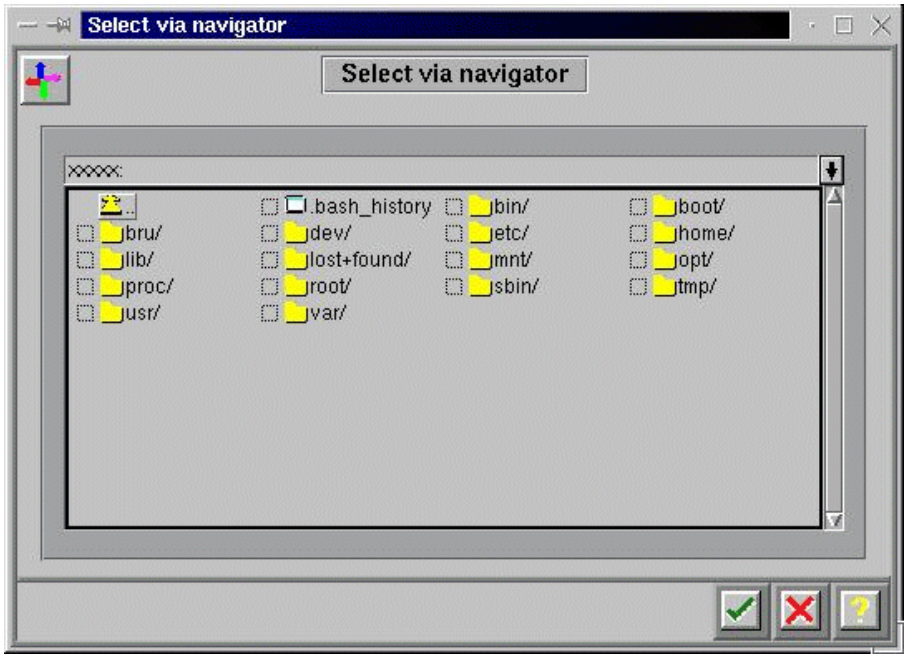


Figure 248. Updated navigator window

To return to the savepacks management window, click the **OK** button. You will see a window similar to Figure 249.

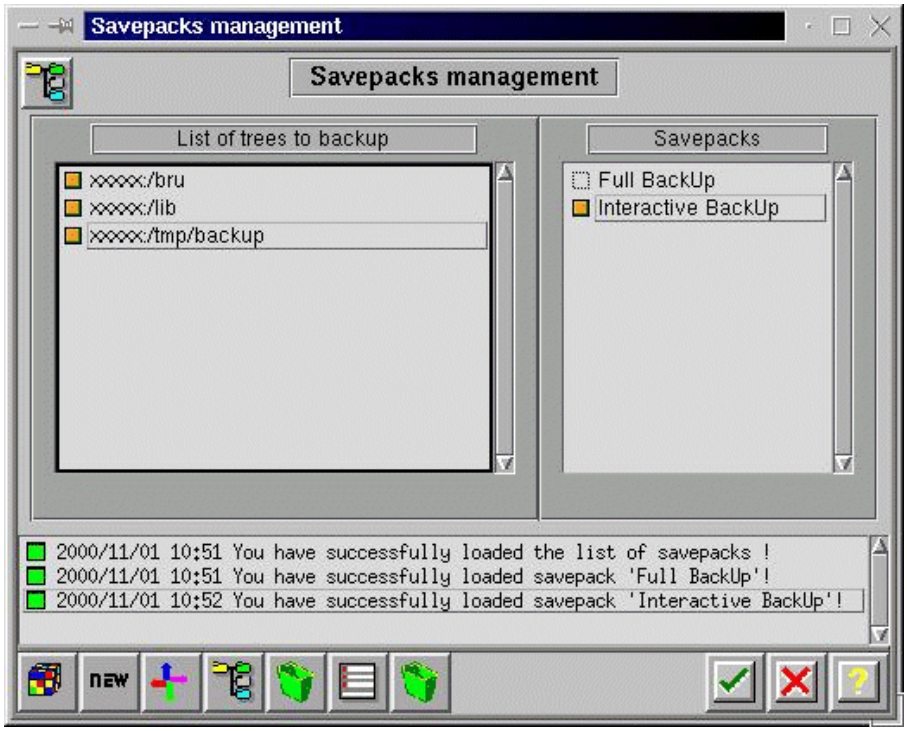


Figure 249. Updated savepacks management window

The basic configuration steps are now done.

Read the *Administrator's Manual* to get more information about the advanced possibilities of Arkeia.

7.3.3 Interactive backup

To start an interactive backup, click the interactive backup button or click **Backup>Interactive Backup** on the menu. A window like Figure 250 appears.

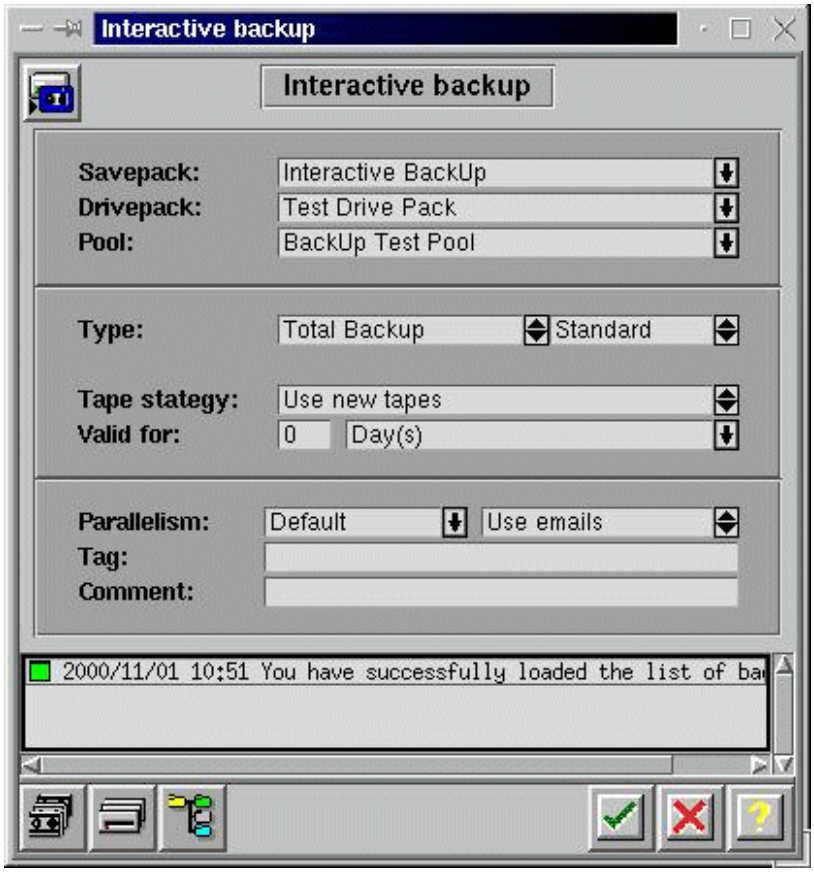


Figure 250. Interactive backup start window

In the comboboxes Savepack, Drivepack and Pool fields, choose which data sets should be backed up on which tapes and on which tape drives.

In the Type box, choose between **Total Backup** and **Incremental Backup** and between **Standard** and **Continous**.

In the Tape Strategy field, choose between **Use new tapes** and **Complete existing tapes**.

In the Valid for field, decide how long the tape(s) for this backup should be valid.

Click the **OK** button to proceed. A window as in Figure 251 appears.

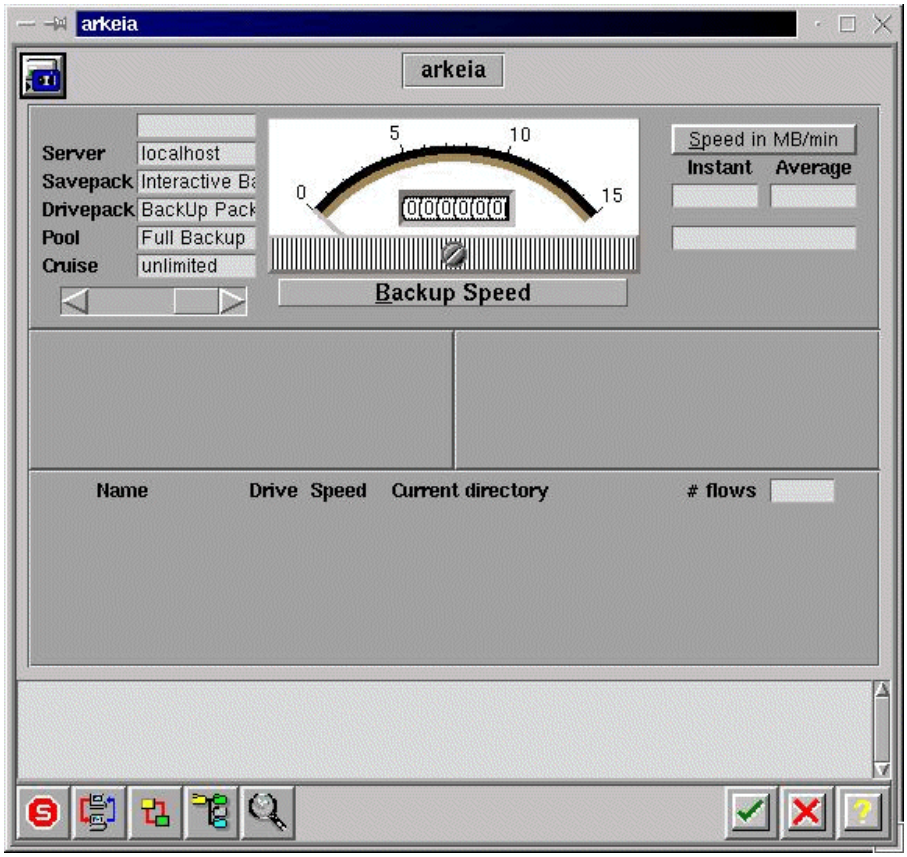


Figure 251. Arkeia's main window during backup

As the backup process proceeds, the content of this window will change. Most of the time, you will see a window like Figure 252.

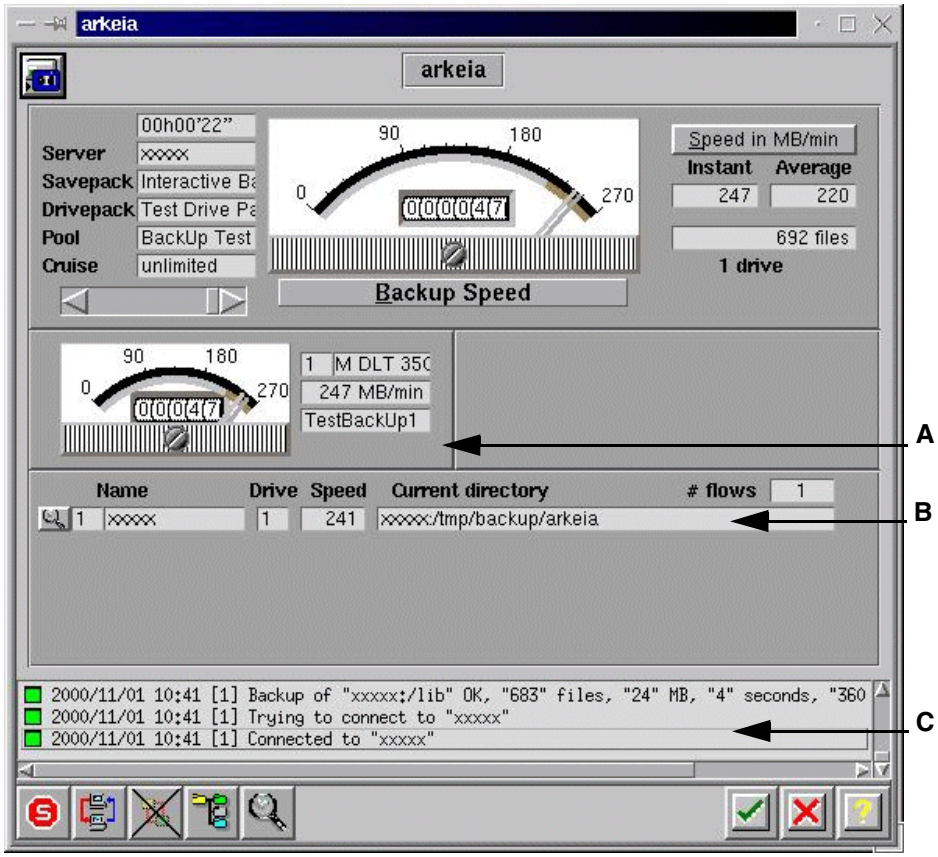


Figure 252. Main window during backup in progress

There are three areas in the window, marked **A**, **B** and **C** in Figure 252, which may require your attention:

In the area pointer **A** points to, you may sometimes see a push button labeled **OK**. Click this button when you have done the action, which was requested in the scroll list area **C**. In the line pointed to by **B**, you see the name of the file that actually is backed up.

You can leave this window by clicking the **OK** button. The backup process continues in the background.

If you want to connect again to this process or - as Arkeia calls it - job, go to Arkeia's main dialog window as shown in Figure 234. In this window you will see a box labeled either "No job running" or "List of jobs". If you see the text "List of jobs" and one or more lines under this box, move the cursor over the

line with the job you want to connect to and press the right mouse button. A pull-down menu as shown in Figure 253 appears.

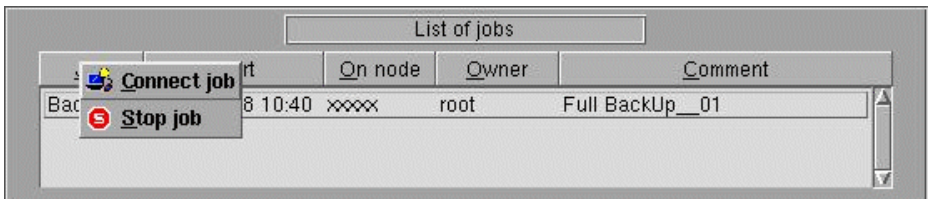


Figure 253. Connect job pull-down menu

Move the cursor over the line with the action you will perform and click the left mouse button. The requested action will be performed.

If you chose **Stop job**, you are asked in a new dialog whether you really want to stop this job.

If you select **Connect job**, you will see a window similar to Figure 252 again.

7.3.4 Periodic Backup

To configure your scheme for periodic backups, press the periodic backup button or go to **Utilities>Periodic Backup** on the menu. You will see a window similar to Figure 254.

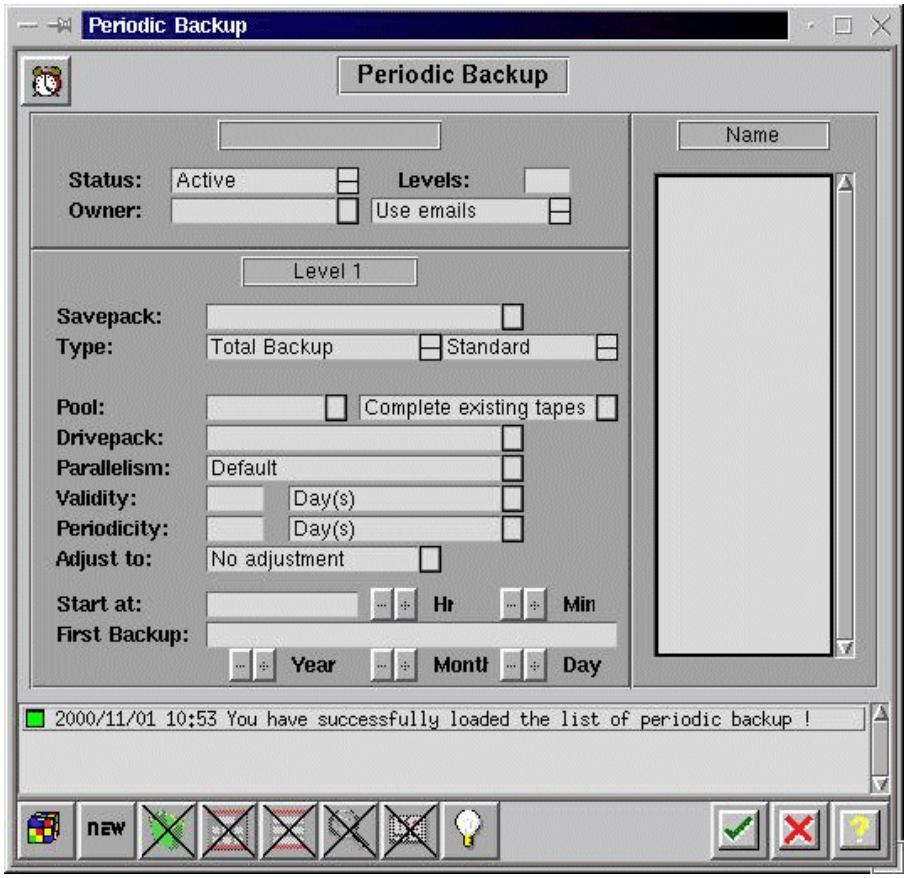


Figure 254. Periodic Backup window

To create a new entry for periodic backup, click the **new** button. You can now fill in the fields with the appropriate information. For more details, please consult the *Administrator's Manual*.

7.3.5 Restoration

To start restoration of data, click the restoration button or click **Restoration -> Restoration** on the menu. You will see a window like Figure 255.

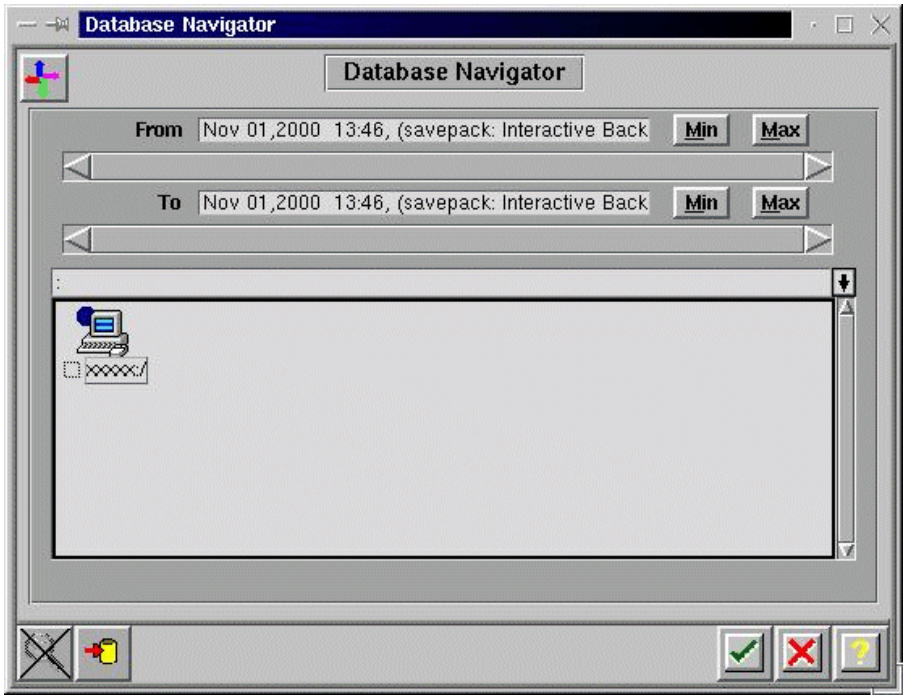


Figure 255. Restoration start dialog

Clicking with the left mouse button over the checkbox beside an item toggles the status of item between selected/not selected. By double-clicking over a symbol for a complete system or a directory, you can navigate through the tree of information that this backup contains. If you are ready with your selection, click the **OK** button and a window like Figure 256 appears, containing a list of the files or directories that will be restored.

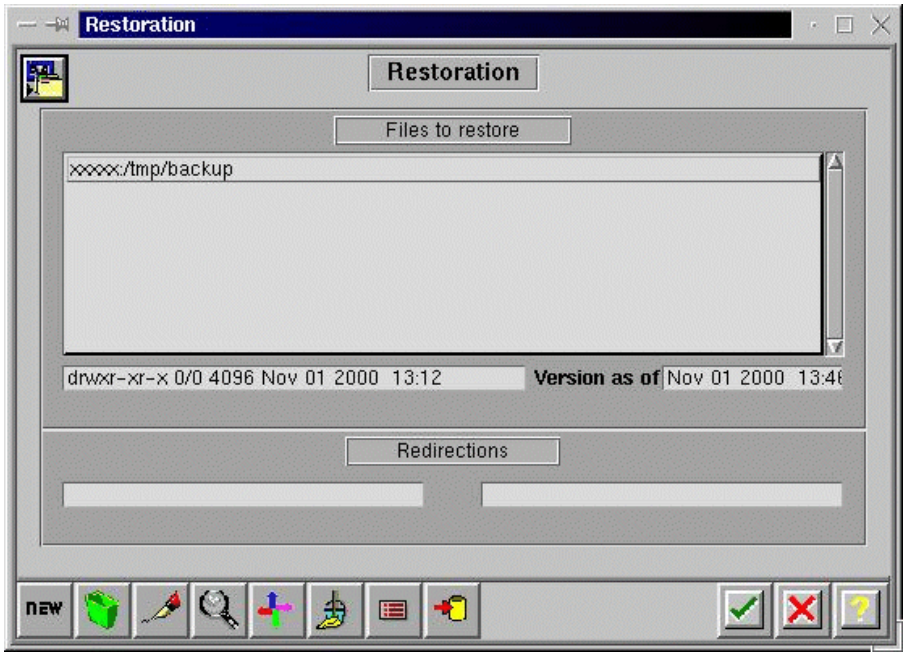


Figure 256. List of directories/files to store

Clicking the **OK** button in this window opens a new window, shown in Figure 257.

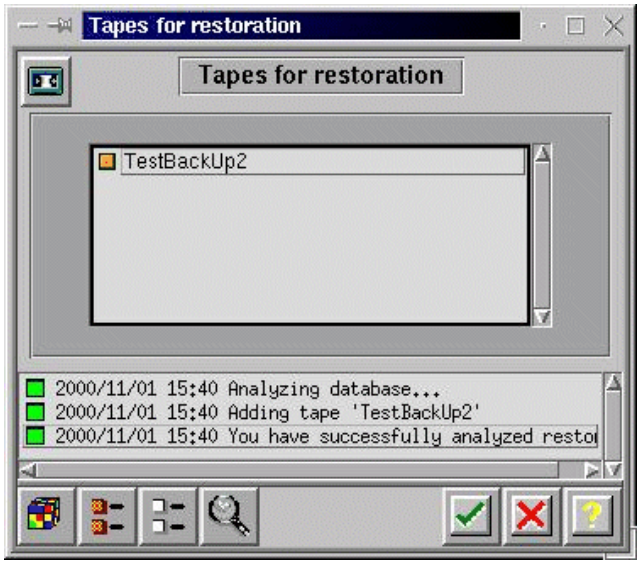


Figure 257. List of tapes used for restoration

You will see a list of the tape(s) that will be used during restoration. Click the **OK** button to proceed.

If the correct tape is already loaded to start the restoration with, you will see a window like Figure 258.

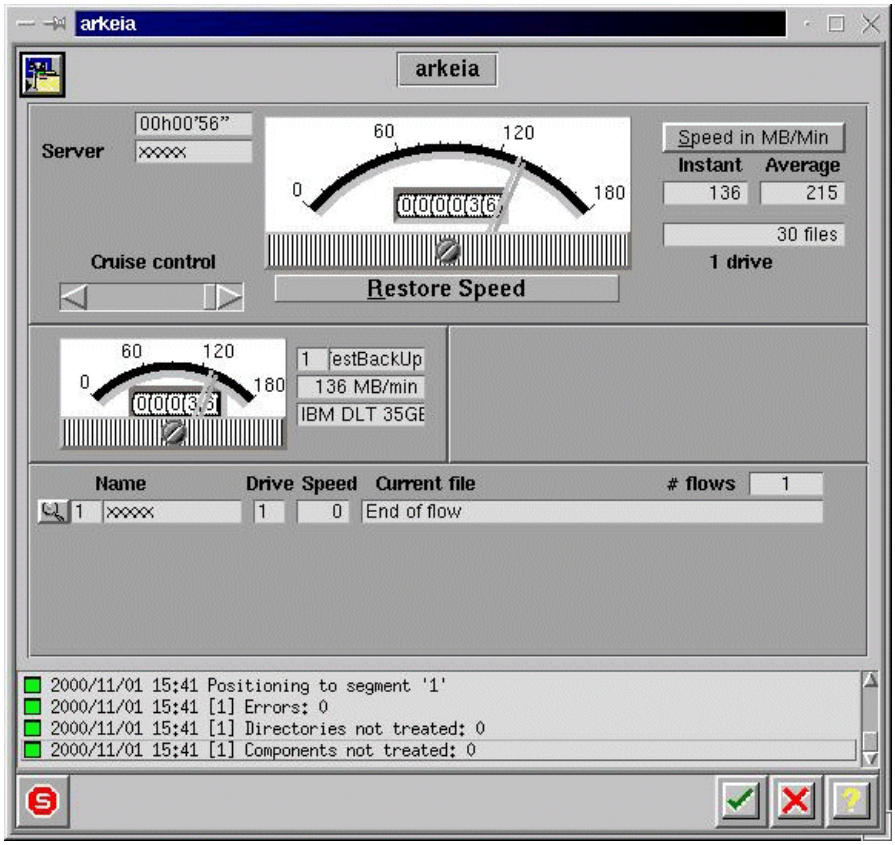


Figure 258. Restoration's main window

If the tape to start with must be mounted, a window like Figure 259 appears.

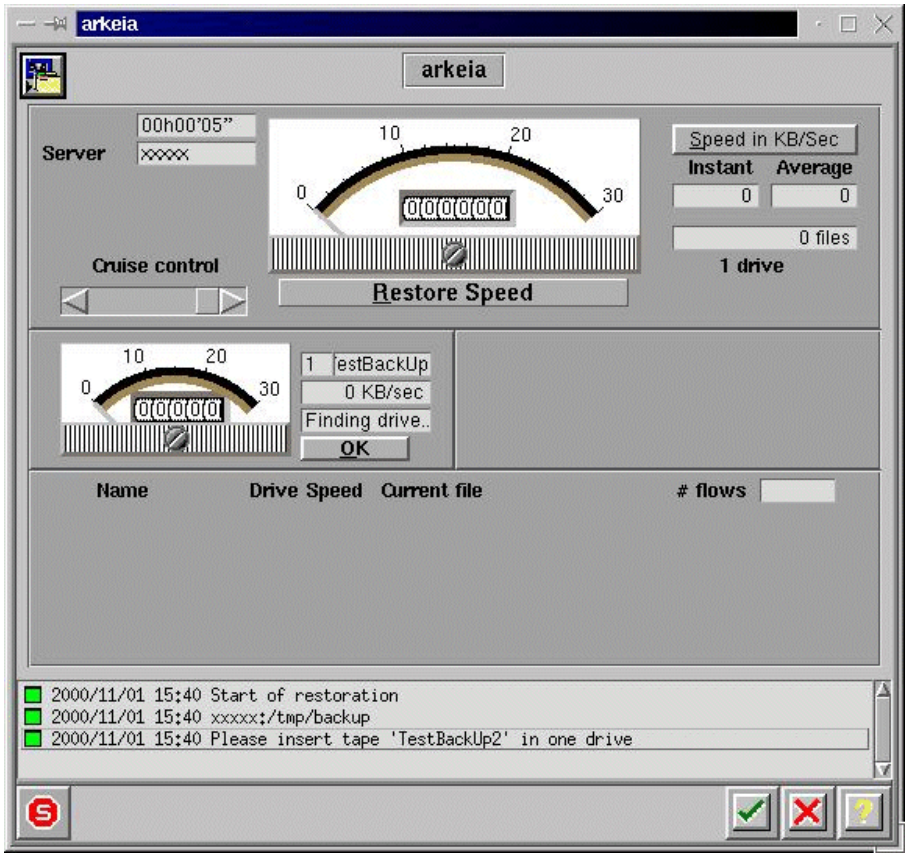


Figure 259. Window during restoration if manual intervention is required

Perform the action required and click **OK** to proceed. The appearance of the window changes. It is now like Figure 258.

7.3.6 Advanced features of Arkeia

For the advanced features of Arkeia, for example how to recycle or label tapes, please read the *Administrator's Manual*.

For more information, consult Arkeia's Web site at:

`http://www.arkeia.com`

Appendix A. Special notices

This publication is intended to help anyone wanting to know more about basic systems administration and backup on the Linux products supported on IBM @server xSeries and Netfinity hardware. The information in this publication is not intended as the specification of any programming interfaces that are provided by IBM @server xSeries and Netfinity. See the PUBLICATIONS section of the IBM Programming Announcement for IBM @server xSeries and Netfinity for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee

© Copyright IBM Corp. 2001

that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

e (logo)® 
IBM ®
Netfinity
NetVista
ServeRAID
xSeries
Redbooks
Redbooks Logo 
WebSphere
Lotus
Domino
Notes

The following terms are trademarks of other companies:

Tivoli, Manage. Anything. Anywhere.,The Power To Manage., Anything. Anywhere.,TME, NetView, Cross-Site, Tivoli Ready, Tivoli Certified, Planet Tivoli, and Tivoli Enterprise are trademarks or registered trademarks of Tivoli Systems Inc., an IBM company, in the United States, other countries, or both. In Denmark, Tivoli is a trademark licensed from Kjøbenhavns Sommer - Tivoli A/S.

C-bus is a trademark of Corollary, Inc. in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

PC Direct is a trademark of Ziff Communications Company in the United States and/or other countries and is used by IBM Corporation under license.

ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States and/or other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Caldera, the C-logo, OpenLinux, COAS, and DR-DOS are either registered trademarks or trademarks of Caldera Systems, Inc.

SuSE and its logo are registered trademarks of SuSE AG.

Linux is a trademark of Linus Torvalds.

Red Hat, RPM, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries.

TurboLinux and its logo are trademarks of TurboLinux, Inc.

Arkeia is a registered trademark of Knox Software.

BRU and QuickStart are registered trademarks of EST, Inc.

BackupEDGE, RecoverEDGE, RecoverEDGE 2 and AdvantEDGE Series are trademarks of Microlite Corporation.

Other company, product, and service names may be trademarks or service marks of others.

Appendix B. Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

B.1 IBM Redbooks

For information on ordering these publications see “How to get IBM Redbooks” on page 259.

- *Linux for WebSphere and DB2 Servers,* SG24-5850
- *Red Hat Linux Integration Guide for IBM @server xSeries and Netfinity*, SG24-5853
- *SuSE Linux Integration Guide for IBM @server xSeries and Netfinity*, SG24-5863
- *TurboLinux Integration Guide for IBM @server xSeries and Netfinity*, SG24-5862
- *Caldera OpenLinux Integration Guide for IBM @server xSeries and Netfinity*, SG24-5861
- *Netfinity Tape Solutions*, SG24-5218
- *Linux on IBM Netfinity Servers: A Collection of Papers*, SG24-5994
- *Lotus Domino R5 for Linux on IBM Netfinity Servers*, SG24-5968
- *Linux Web Hosting with WebSphere, DB2, and Domino*, SG24-6007

B.2 IBM Redbooks collections

Redbooks are also available on the following CD-ROMs. Click the CD-ROMs button at ibm.com/redbooks for information about all the CD-ROMs offered, updates and formats.

CD-ROM Title	Collection Kit Number
IBM System/390 Redbooks Collection	SK2T-2177
IBM Networking Redbooks Collection	SK2T-6022
IBM Transaction Processing and Data Management Redbooks Collection	SK2T-8038
IBM Lotus Redbooks Collection	SK2T-8039
Tivoli Redbooks Collection	SK2T-8044
IBM AS/400 Redbooks Collection	SK2T-2849
IBM Netfinity Hardware and Software Redbooks Collection	SK2T-8046
IBM RS/6000 Redbooks Collection	SK2T-8043
IBM Application Development Redbooks Collection	SK2T-8037

© Copyright IBM Corp. 2001

CD-ROM Title	Collection Kit Number
IBM Enterprise Storage and Systems Management Solutions	SK3T-3694

B.3 Other resources

These publications are also relevant as further information sources and can be viewed at `http://www.linuxdoc.org`:

- *The Linux System Administrators' Guide*
- *Linux Administration Made Easy*
- *Linux Documentation Project*
- *Running Linux*

B.4 Referenced Web sites

These Web sites are also relevant as further information sources:

- `http://www.linuxdoc.org/` LDP documentation
- `http://www.sunsite.unc.edu/LDP/` LDP documentation
- `http://www.arkeia.com/` Arkeia backup product for Linux
- `http://www.estinc.com/` BRU/CRU backup product for Linux
- `http://www.microlite.com/` BackupEDGE backup product for Linux
- `http://www.calderasystems.com/` Caldera OpenLinux Web site
- `http://www.redhat.com/` Red Hat Linux Web site
- `http://www.suse.com/` SuSE Linux Web site
- `http://www.turbolinux.com/` TurboLinux Web site
- `http://www.redbooks.ibm.com/` IBM Redbooks Web site
- `http://www.ibm.com/storage/` IBM Storage Solutions
- `http://www.coas.org/index.html/` Caldera Open Administration System
- `http://www.kde.org/` KDE Window Manager Web site
- `http://www.rpm.org/` Red Hat Package Manager Web site
- `http://solucorp.qc.ca/linuxconf/` Linuxconf utility

How to get IBM Redbooks

This section explains how both customers and IBM employees can find out about IBM Redbooks, redpieces, and CD-ROMs. A form for ordering books and CD-ROMs by fax or e-mail is also provided.

- **Redbooks Web Site** ibm.com/redbooks

  Search for, view, download, or order hardcopy/CD-ROM Redbooks from the Redbooks Web site. Also read redpieces and download additional materials (code samples or diskette/CD-ROM images) from this Redbooks site.

  Redpieces are Redbooks in progress; not all Redbooks become redpieces and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

- **E-mail Orders**

  Send orders by e-mail including information from the IBM Redbooks fax order form to:

	e-mail address
In United States or Canada	pubscan@us.ibm.com
Outside North America	Contact information is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Telephone Orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	Country coordinator phone number is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Fax Orders**

United States (toll free)	1-800-445-9269
Canada	1-403-267-4455
Outside North America	Fax phone number is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl

This information was current at the time of publication, but is continually subject to change. The latest information may be found at the Redbooks Web site.

IBM Intranet for Employees

IBM employees may register for information on workshops, residencies, and Redbooks by accessing the IBM Intranet Web site at http://w3.itso.ibm.com/ and clicking the ITSO Mailing List button. Look in the Materials repository for workshops, presentations, papers, and Web pages developed and written by the ITSO technical professionals; click the Additional Materials button. Employees may access MyNews at http://w3.ibm.com/ for redbook, residency, and workshop announcements.

© Copyright IBM Corp. 2001

IBM Redbooks fax order form

Please send me the following:

Title	Order Number	Quantity

First name	Last name	
Company		
Address		
City	Postal code	Country
Telephone number	Telefax number	VAT number

☐ Invoice to customer number _____

☐ Credit card number _____

Credit card expiration date	Card issued to	Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

Index

© Copyright IBM Corp. 2001

P

R

S

T

U

X

Y

Z

IBM Redbooks review

Your feedback is valued by the Redbook authors. In particular we are interested in situations where a Redbook "made the difference" in a task or problem you encountered. Using one of the following methods, **please review the Redbook, addressing value, subject matter, structure, depth and quality as appropriate.**

- Use the online **Contact us** review redbook form found at **ibm.com**/redbooks
- Fax this form to: USA International Access Code + 1 845 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Document Number **Redbook Title**	SG24-6228-00 Linux System Administration and Backup Tools for IBM @server xSeries and Netfinity
Review	
What other subjects would you like to see IBM Redbooks address?	
Please rate your overall satisfaction:	O Very Good O Good O Average O Poor
Please identify yourself as belonging to one of the following groups:	O Customer O Business Partner O Solution Developer O IBM, Lotus or Tivoli Employee O None of the above
Your email address: The data you provide here may be used to provide you with information from IBM or our business partners about our products, services or activities.	O Please do not use the information collected here for future marketing or promotional contacts or other communications beyond the scope of this transaction.
Questions about IBM's privacy policy?	The following link explains how we protect your personal information. **ibm.com**/privacy/yourprivacy/

© Copyright IBM Corp. 2001

Linux System Administration and Backup Tools for IBM @server xSeries and Netfinity

(0.5” spine)
0.475”<->0.875”
250 <-> 459 pages

Linux System Administration and Backup Tools

for IBM @server xSeries and Netfinity

The complete guide for system administration tools and choosing the appropriate backup solution for your Linux OS on xSeries and Netfinity

Step-by-step basic system administration instructions for Caldera, SuSE, Red Hat, and TurboLinux

Install and configure Arkeia, BRU, and BackupEDGE for Linux

This redbook gives you an understanding of the unified system administration incorporated in the Caldera OpenLinux, Red Hat Linux, SuSE Linux and TurboLinux operating systems. It also provides information on three Linux backup and recovery applications supported by these operating systems.

This redbook provides an understanding of Linux system administration and backup at a fairly detailed level, to help you increase your Linux skills in both areas quickly and easily.

This redbook also directs you to the available IBM Redbooks of Caldera OpenLinux, Red Hat Linux, SuSE Linux and TurboLinux that provide specific global instructions to help you plan, install, and configure each operating system on IBM @server xSeries and Netfinity for satisfactory operation.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-6228-00 ISBN 0738422487